AI & The Future of Healthcare

Innovation, Risk, and Real-World Impact

A panel discussion on deployment, governance, contracting, and the legal landscape shaping healthcare AI today.

Healthcare AI: Core Use Cases

Three categories — each triggers different regulatory, liability, and governance requirements

Clinical & Patient-Facing

- **Clinical Decision Support**
  AI-assisted diagnosis, imaging analysis, treatment recommendations
- **Diagnostic Imaging AI**
  Radiology, pathology slide review, ECG interpretation
- **Predictive Risk Scoring**
  Sepsis alerts, readmission risk, deterioration flags
- **Ambient Documentation**
  AI scribes auto-generating clinical notes

Revenue & Operational

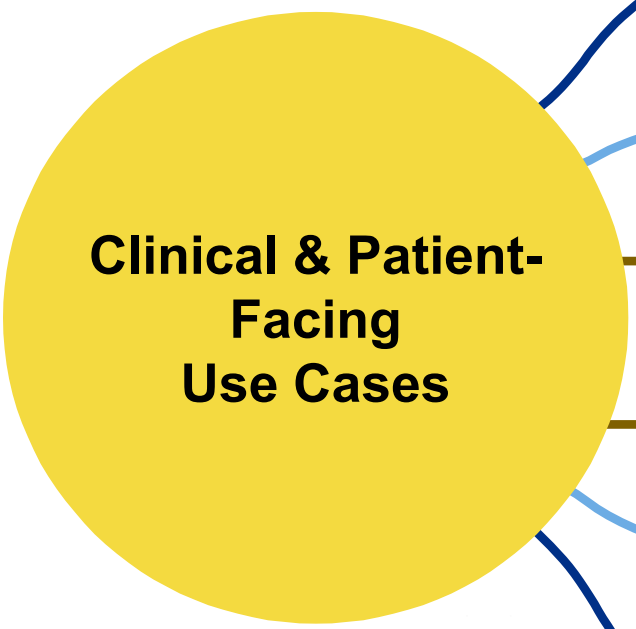
- **Prior Authorization**
  Automated coverage determinations — most heavily regulated
- **Revenue Cycle & Coding**
  Computer-assisted coding, claim scrubbing, denial prediction
- **Administrative Automation**
  Scheduling, staffing optimization, referral management
- **Population Health**
  Care gap analysis, utilization modeling, risk stratification

Data, Platform & Infrastructure

- **Fraud, Waste & Abuse**
  Network anomaly detection, referral and kickback alerts
- **Cybersecurity AI**
  Intrusion detection, malware and phishing identification
- **EHR Integration Layers**
  AI embedded in Epic, Oracle Cerner, and other platforms
- **Analytics Infrastructure**
  Readmission prediction, risk stratification, benchmarking

Healthcare AI:
Clinical & Patient-Facing

AI that influences diagnosis, treatment, triage, or clinical decision-making



CLINICAL DECISION SUPPORT (CDS)
AI-assisted diagnosis, triage tools, treatment recommendations, risk stratification

DIAGNOSTIC IMAGING & SIGNAL ANALYSIS
Radiology image analysis, pathology slide review, ECG interpretation

PREDICTIVE ANALYTICS & RISK SCORING
Sepsis prediction, patient deterioration alerts, readmission risk

EMERGENCY & DISPATCH SETTINGS
AI-assisted EMS dispatch, acuity prioritization, destination decision support

REMOTE PATIENT MONITORING AND WEARABLES
AI interpretation of device data, anomaly detection

PATIENT ENGAGEMENT & VIRTUAL ASSISTANTS
Symptom checkers, chatbots, care navigation tools

Healthcare AI:
Revenue & Operational

AI that affects billing, reimbursement, financial performance, or administrative workflows

REVENUE CYCLE & FINANCIAL
Coding authorization, billing optimization, prior authorization, utilization management, claims denial and management

ADMINISTRATIVE WORKFLOW AUTOMATION
Scheduling, patient capacity, staffing optimization, referral workflows

POPULATION HEALTH & ANALYTICS
Care gap analysis, utilization modeling

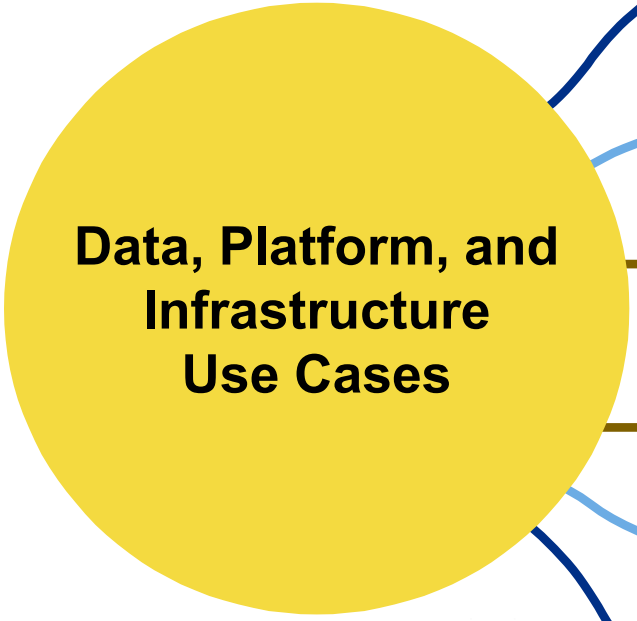
PATIENT ENGAGEMENT
Appointment and medication reminders, benefits navigation, referral and care navigation

SUPPLY CHAIN & LOGISTICS
Inventory forecasting, vendor optimization

PRICE ESTIMATION & PATIENT COST-SHARING
Cost prediction, out-of-pocket estimates, service pricing

Healthcare AI:
Data, Platform, and Infrastructure

AI that enables or supports other systems but may not directly touch patient care or revenue



MODEL TRAINING
Diagnostic imaging, lab value prediction, patient clustering, anomaly detection

DATA LABELING AND ANNOTATION TOOLS
Medical imaging annotation, structured data labeling platforms, audio/speech annotation

POPULATION HEALTH & ANALYTICS
Hospital readmission prediction, risk stratification for disease management, preventative care, SDoH analytics

FRAUD, WASTE, AND ABUSE DETECTION
Automated claims review, outlier provider detection, risk scoring of claims, referral/kickback detection

CYBERSECURITY AND ANOMOLY DETECTION
Network intrusion detection, malware and phishing detection, unauthorized access alerts

MARKETING
Targeted email/text campaigns, social media engagement, chatbots and virtual assistants

Key Risks: Healthcare AI

Every deployment decision is also a risk decision

Bias & Discrimination

HIGH

AI trained on non-representative data perpetuates disparate outcomes by race, gender, and socioeconomic status. Triggers Section 1557 and state algorithmic discrimination statutes.

State AI Laws

Liability & Malpractice

HIGH

When AI-assisted clinical decisions lead to patient harm, liability allocation remains unsettled. Learned intermediary doctrine and product liability theories are actively being litigated.

Malpractice · Product Liability

Privacy & Data Security

HIGH

Training AI on PHI triggers HIPAA obligations. De-identification is complex — re-identification risk is real. State laws (CMIA, SHIELD Act) impose stricter requirements beyond HIPAA.

HIPAA · State Privacy Laws

Regulatory Non-Compliance

HIGH

AI deployed without FDA clearance, off-label use of cleared devices, and failure to maintain post-market surveillance create substantial enforcement exposure for providers and developers.

FDA · CMS · OIG

Transparency & Explainability

MED

Black-box AI makes it difficult to explain clinical decisions to patients and regulators. FDA, ONC HTI-1, and state laws impose explainability requirements for high-risk AI systems.

State Disclosure Laws

Informed Consent & Autonomy

MED

Patients may not know AI is involved in their care. California AB 3030 and pending state laws require disclosure when AI generates patient communications or informs clinical decisions.

Patient Rights

Best Practices:
Good, Better, Best Governance Practices

GOOD

- **Goal: Avoid obvious regulatory and enforcement failures**
  - **AI Inventory:** Maintain basic inventory of AI tools in use (clinical, operational, patient-facing, data/analytics)
  - **Human Oversight:** Ensure humans review AI outputs that affect care, billing, or patients
  - **Privacy & Security:** Apply HIPAA Security Rule safeguards to AI systems handling PHI
  - **Vendor Diligence:** Confirm AI vendors' compliance claims (HIPAA, security certifications)
  - **Disclosure:** Provide required disclosures when AI is used in patient communications

BETTER

- **Goal: Withstand audits, diligence, and enforcement inquiry**
  - **AI Governance Committee:** Cross-functional oversight (legal, clinical, compliance, IT, security)
  - **Use-Case Risk Classification:** Distinguish clinical vs. non-clinical vs. patient-facing AI
  - **Pre-Deployment Risk Assessments:** Bias, safety, accuracy, and misuse analysis
  - **Model Documentation:** Intended use, limitations, training data sources, performance metrics
  - **Monitoring & Change Management:** Track model drift, retraining, and version control
  - **Clear Accountability:** Defined owners for AI decisions and incident escalation

BEST

- **Goal: Proactively reduce enforcement risk and support growth**
  - **Formal AI Governance Framework:** Aligned to NIST AI RMF, FDA SaMD principles, and DOJ compliance guidance
  - **Human-in-the-Loop by Design:** Documented clinical override authority and escalation paths
  - **Continuous Validation:** Ongoing bias testing, safety review, and outcome measurement
  - **Audit-Ready Evidence:** Logs, model decisions, overrides, and monitoring reports
  - **Integrated M&A & Product Governance:** AI risk review embedded in product launches and acquisitions
  - **Board Reporting:** Regular AI risk, compliance, and performance updates

Best Practices:
Practical Takeaways

- **Define Intended Use and Customer Reliance**
  - — Be explicit about what your AI is designed to do, who should rely on it, and who should not — ambiguity drives FDA, FTC, and contract risk.
- **Segment Products by Risk Profile**
  - — Clearly distinguish clinical decision support, patient-facing functionality, and operational analytics within your platform; apply different controls and messaging to each.
- **Design Human-in-the-Loop by Default**
  - — Ensure customers can review, validate, and override AI outputs; avoid workflows that encourage blind reliance.
- **Document Limitations and Guardrails**
  - — Provide plain-language disclosures on accuracy, bias, training data limitations, and appropriate use — and keep them consistent across marketing, contracts, and UI.
- **Treat AI Output as Regulated Content**
  - — Assume AI-generated documentation, recommendations, and messages may be reviewed by regulators, auditors, or litigants.
- **Operationalize Monitoring and Change Control**
  - — Track model performance, drift, retraining, and version changes; communicate material changes to customers in advance.
- **Align Vendor and Sub-Vendor Risk**
  - — Flow down security, privacy, audit, and incident-reporting obligations to model providers, cloud platforms, and data partners.
- **Build Governance That Scales With Customers**
  - — Design governance processes that support enterprise customers, audits, and diligence — not just product launches.