Welcome to Clark Hill's 3rd Annual Healthcare Symposium

Dallas, Texas

February 4, 2026

1

Today's Agenda

5:30 PM	**Welcome Remarks**
5:35 – 6:00	**Consenting to Connect: How Telehealth Bridges Digital Health and AI Companies into HIEs**
6:00 – 6:25	**Charting the Future: Legal Considerations for Healthcare Professionals in the Age of AI**
6:25 – 6:45	**Summary of 2025 Government Healthcare Investigations, Enforcement Actions and Anticipated Priorities for 2026**
6:45 – 7:00	**Dinner**
7:00 – 7:20	**From Information Blocking to Sharing: Operationalizing the 21st Century Cures Act in Hospitals and Clinics**
7:20 – 7:50	**Healthcare Provider Panel: Texas Non-Compete Law**
7:50 – 8:00	**Wrap Up + Closing Remarks**

2

Section 1 (5:35 – 6:00)

Consenting to Connect: How Telehealth Bridges Digital Health and AI Companies into HIEs

Presented by: Tim McGibboney, Senior Attorney, Healthcare

clarkhill.com

3

Why This Matters Now (2026)

- Digital health & AI companies need longitudinal, multi-source health data to move beyond demos or curated applications
- Information blocking enforcement + TEFCA push raise the stakes
- Consumer privacy expectations rising; consent UX is strategic
- Payer/provider 'digital front doors' compete for patient trust
- Investors demand data ROI and defensible compliance posture

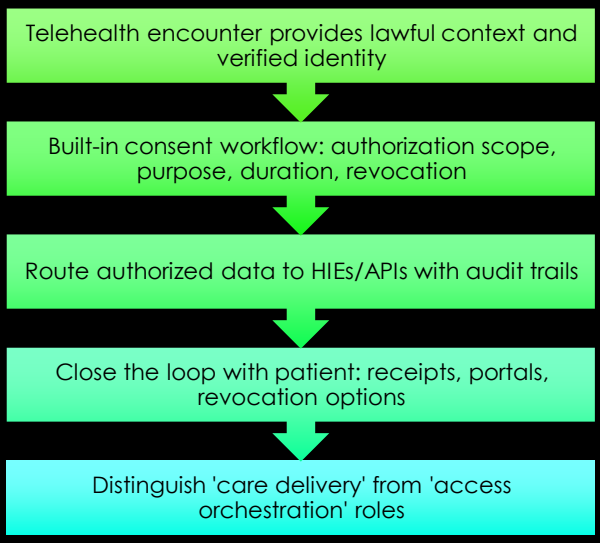
4

The Structural Problem

- Traditional pathways, dilemma, & current rules
- CPOM limits non-physician control over medical practice and clinical decisions
- HIE participation is often gated by provider status and contractual frameworks
- Consent capture is fragmented and inconsistent across touchpoints
- Payer/provider/tech silos + variable state law create friction
- **Result**: lawful, scalable data access is slow and brittle

5

The Solution: Telehealth as the Front Door



6

MSO/PSA Model: CPOM-Safe Scaffolding

Physician entity owns practice; independent medical judgment preserved

MSO provides non-clinical: admin, tech, staffing, revenue cycle, facilities

PSA defines professional services, supervision, and quality oversight

Cash pay; Insurance; FHCP Business
FMV and commercial reasonableness; no volume/value of referrals

Clear segregation of control: tech/ops vs. clinical decision-making

7

CPOM Variability: 50-State Glance

Stricter states (e.g., CA, TX) vs. more flexible regimes

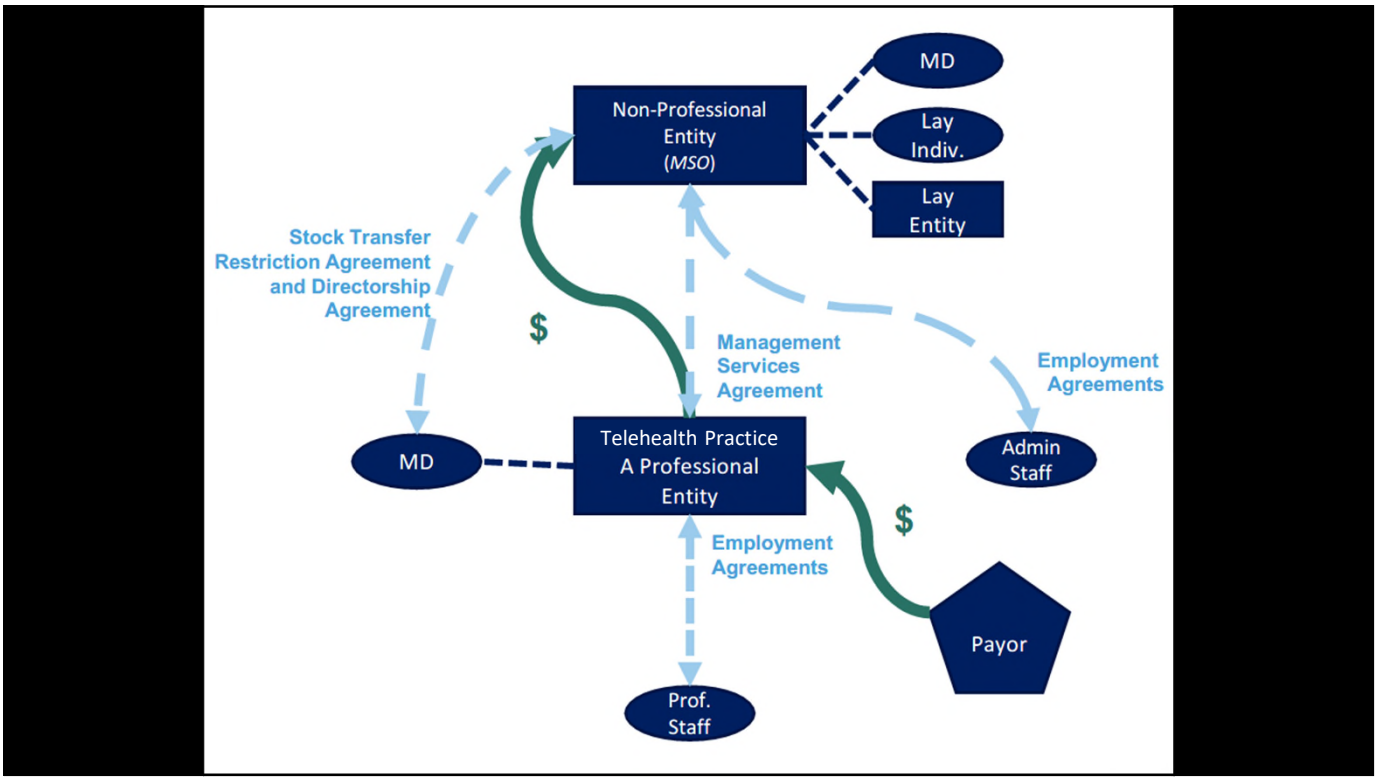
Professional entities: PCs, PLLCs, PAs; ownership and director rules

Restrictions: fee-splitting, lay control, supervision mandates

Licensure/telehealth registration overlays for multi-state models

Coordinate local counsel; adapt MSO/PSA templates per state

8



9

Consent Mechanics: From Click to HIE

- Identity proofing: KBA, government ID, in-encounter verification
- Authorization scope & purpose: specificity beats boilerplate
- Revocation: easy, logged, and propagated to downstream systems
- Retention & auditability: timestamps, versions, event trails
- Edge cases: minors/guardians, POA, incapacitated patients

10

Consent as Compliance Shield & Asset

- HIPAA: TPO (use or disclose) vs. patient authorization—know the difference
- HITECH strengthens HIPAA enforcement; document authorizations
- 42 CFR Part 2 caveats for SUD information; additional consent layers
- Contractual data rights/licensing tied to consent status and scope
- Renewal and churn metrics: consent as a measurable market asset (investor diligence)

11

Telehealth → Data → (AI) Pipeline

- Event capture from encounters; normalization & mapping (USCDI, FHIR)
- De-identification/pseudonymization with re-link under authorization
- Model training/inference with guardrails (DUAs/BAAs, role-based access)
- Feedback to clinicians/patients; continuous improvement loop
- Latency & volume targets: plan for scale from day one

12

Risk Hotspots & Mitigations

- AKS/Stark: remuneration/referrals; apply safe harbors/exceptions
- Fee-splitting and lay influence over clinical judgment—firewalls
- Information blocking & TEFCA participation duties—don't obstruct
- State privacy (e.g., CCPA/CPRA) + sectoral laws; honor rights
- Security: least privilege, audits, incident response, vendor diligence

13

Contracting Checklist (MSO/PSA & HIE)

FMV & commercial reasonableness attestations; compensation mechanics

Data rights: license scope, de-ID rights, derivatives, termination wind-down

HIPAA BAAs, DUAs, and Part 2 Qualified Service Agreements as needed

Audit rights, SLAs, security exhibits, change control boards

Termination triggers: consent changes, regulatory shifts, breaches

14

Sensitive Data & Special Cases

- 42 CFR Part 2 SUD records: stricter consent and redisclosure limits
- Reproductive and other sensitive services: heightened privacy concerns
- Minors/guardianship and cross-jurisdictional consent mismatches
- Out-of-state telehealth licensure and supervision considerations
- Segment & isolate flows; apply higher bars where warranted

15

Operating Model & Governance

- Consent registry and dashboard; revocation latency KPI (time taken to effect revocation from receipt)
- DPIAs/TRA; role-based access; periodic access reviews
- Monitoring, audit logging, and independent compliance oversight
- Incident response with regulator and HIE notification playbooks
- Training, attestations, and board-level reporting cadence

16

Future: Consent-Based Ecosystems

- Portable consent wallets and patient-directed exchange at scale
- Interoperability via HIEs/TEFCA and network effects
- Payer–provider–tech data liquidity under patient control
- Telehealth as persistent consent orchestrator across touchpoints
- Speculative but near-term: early pilots already emerging

17

Action Checklist and Q&A

- Validate CPOM posture and entity structuring
- Design a robust consent UX and registry
- Lock down contracts (FMV, BAAs/DUAs, data rights)
- Pilot an HIE integration with clear KPIs
- Measure outcomes; iterate governance and controls

Questions? Contact Tim:
tmcgibboney@clarkhill.com

18

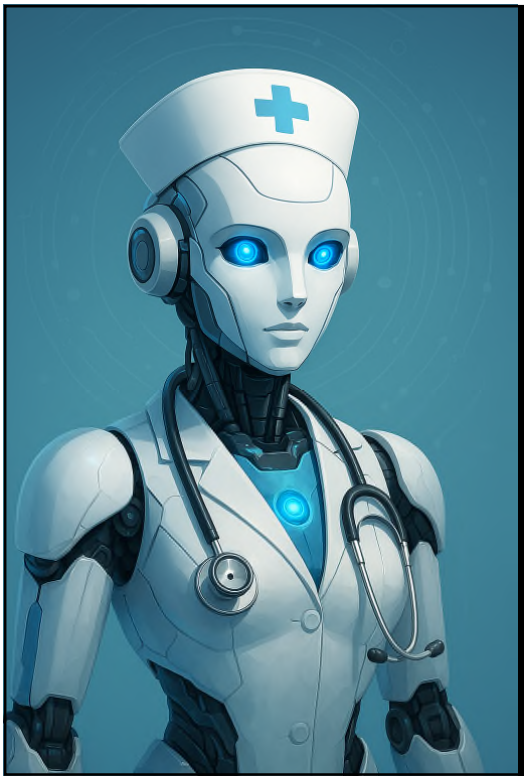
Section 2 (6:00 – 6:25)

Charting the Future: Legal Considerations for Healthcare Professionals in the Age of AI

Presented by: John Howard, Senior Attorney, Cybersecurity and Data Privacy

clarkhill.com

19



Agenda

1. What is AI in Healthcare
2. Risks Associated with AI Use in Healthcare
3. Federal and State Approach to Regulating AI

20

‘We need to design and build AI that helps healthcare professionals be better at what they do. The aim should be enabling humans to become better learners and decision-makers.’

Mihaela van der Schaar, PhD, director of the Cambridge Centre for AI in Medicine at the University of Cambridge in the U.K. (source: The Guardian*)*

‘AI offers great potential, [but] integrating it into medical workflow software requires caution. While potentially impeding progress, government regulations play a crucial role in protecting patients and society.’

Rob Versaw, MBA, vice president of innovation & growth at Envista Holdings (source: Forbes*)*

‘Healthcare providers are increasingly faced with multiple vendors claiming to have AI. To what extent is [each vendor’s] AI learning from your data—or using that data to train models for their other customers?’

Damian Chung, EdD, business information security officer & healthcare CSO at Netskope (source: BankInfoSecurity*)*

21

What is AI

Many forms (machine learning, deep neural networks, natural language processing, etc..) that rely on two basic types.

Generative (Dynamic) AI:

- A type of artificial intelligence technology that can produce various types of content, including text, imagery, audio and synthetic data.
- Generative AI learns the patterns and structure of its training data and generates content with similar characteristics

Analytical (Static) AI:

- “Traditional AI” that focuses on analyzing existing data that can be used for predictions and automation

22

Uses of AI in Healthcare

- Training – scenario simulations
- Clinical Decision / Diagnosis Support
- Resource Allocation
- Customer Service
- Administrative Support
- Workflow design / management
- The list keeps growing…..

23

Examples of AI in Healthcare

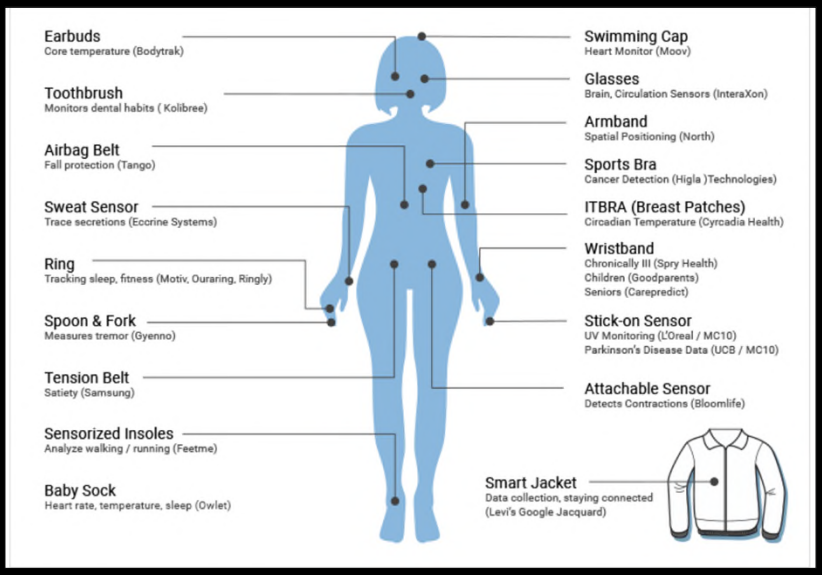
AI Scribes:
- Provides in room assistance in documenting a visit and creating notes
- DeepScribe, RevMaxx

Resource Management:
- Cloud-based resource capacity management, staffing, and patient flow forecasting
- LeanTaaS, iQueue

Consumer Facing Personal Health Records:
- Apps that allow for health tracking, measurement-based recommendations, and education
- Some present options for clinical integrations
- Emagine Solutions Technology, The Journey

24

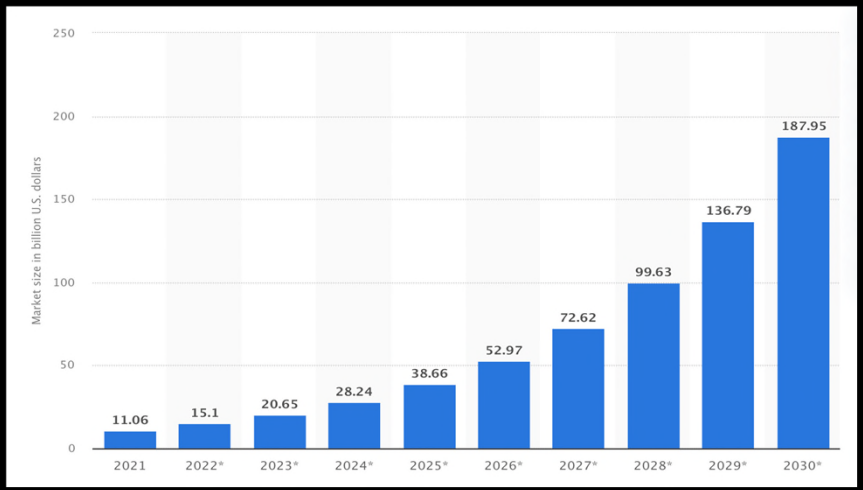
AI Integrations with Internet of Medical Things (IoMT)



25

The AI in healthcare market is projected to grow to $52.97 billion in 2026

https://www.statista.com/statistics/1334826/ai-in-healthcare-market-size-worldwide/



26

Potential Legal Risks

- Malpractice (over reliance on AI determinations)
- Discrimination / Discriminatory Practices (potential for bias in the AI models)

  Alignment Problem by Brian Christian
- Privacy (unauthorized uses or disclosures of health information)
- Cybersecurity (violation of HIPAA security rule, State law, FDA requirements, or other federal regulations)

27

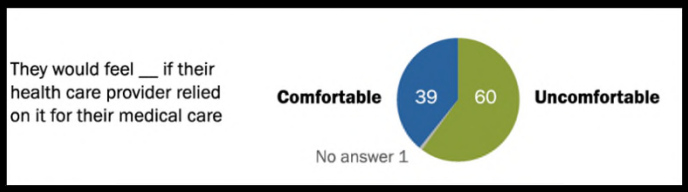
Perceived Risks of AI in Healthcare

- Discrimination, prejudice, or favoritism
- Use of inaccurate or biased data models
- Over reliance
- Changes over time (Generative AI)

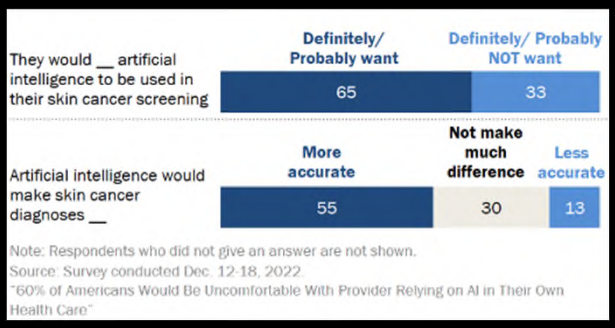
Benefits… more opportunity for efficiency gains and better heath outcomes

28

60% of US adults 'uncomfortable' with healthcare providers relying on AI

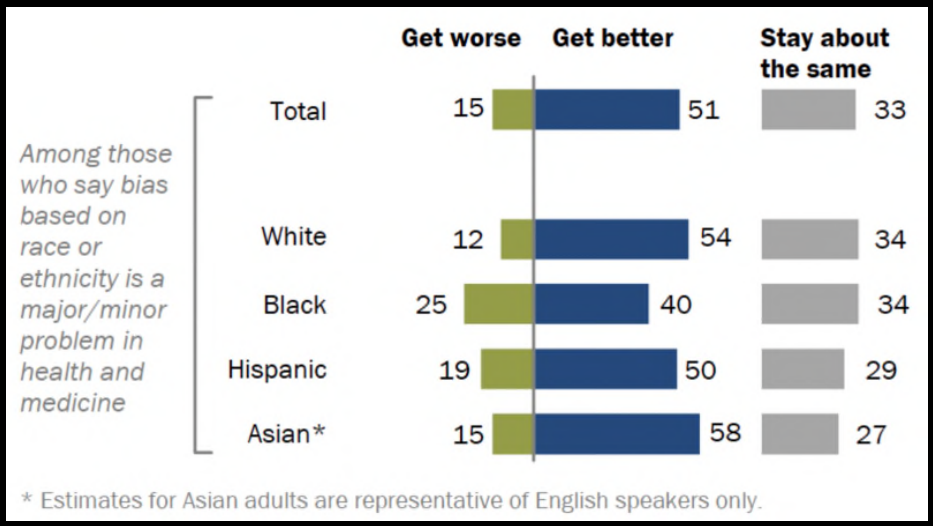


65% of US adults want AI to be used in their cancer screening



29

51% of US adults who say ethnic biases in healthcare are a problem believe AI will reduce bias



30

Federal & State Regulators Target AI

State Level AI task forces: Monitor AI in multiple industries and recommend laws and regulations

- Lawmakers in 46 states have introduced more than 250 bills to regulate AI in healthcare (2025 legislative session)
- Of these, 27 have been enacted across 17 states

Federal Push to promote and control AI innovation

- Federal agencies looking to pre-empt all AI state laws to try and control national approach

31

Why AI Compliance Matters

Non-compliance risks:

- FDA enforcement for unapproved medical devices
- State restrictions on AI-driven clinical decision-making
- Data privacy violations (HIPAA, state AI/privacy laws)
- Scale balancing innovation vs. legal risk

32

FDA Oversight of AI/ML

- AI as a Medical Device: regulated under 21 CFR Part 800–1299
- Risk-based classification (Class I–III) depends on clinical impact
- Key obligations for providers using AI in telehealth:
- Use only FDA-cleared or authorized devices
- Follow manufacturer instructions & maintain logs
- Report adverse events per 21 CFR Part 803 (MDR)
- AI software updates: check whether "locked" vs "adaptive" affects regulatory obligations

33

State AI Laws

California (CDPA/CPRA + AI transparency bills)

- Requirements for explainability, bias mitigation, and data handling

New York, Illinois, Virginia: Emerging AI legislation affecting:

- Clinical decision support transparency
- Patient consent for AI-assisted care

Texas SB 1188 – Permits use of AI for diagnosis or treatment, if:

1. Used within the scope of practitioner's license;
2. Results are reviewed by practitioner; and
3. Use of AI must be disclosed

34

Data Privacy Associated with AI

- AI requires large patient datasets → privacy risks
- Compliance requirements:
- HIPAA: AI data must be de-identified or protected under BAAs
- CPRA, CDPA: AI-generated inferences may be sensitive personal info
- Implement technical/organizational safeguards:
- Access control, audit logging, encryption
- Policies to prevent AI re-identification of de-identified data

35

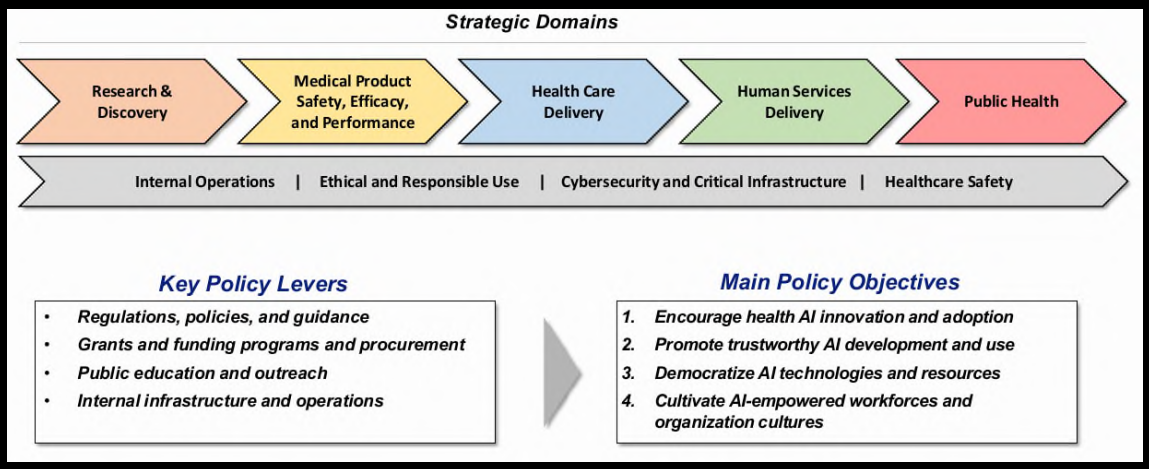
Federal Approach

FAVES Principles

Fair	Does not exhibit prejudice or favoritism toward an individual or group based on their inherent or acquired characteristics
Appropriate	Outputs are well matched to produce results appropriate for specific contexts and populations to which they are applied
Valid	Outputs have been shown to estimate targeted values accurately and as expected in both internal and external data
Effective	Outputs have demonstrated benefits in real-world conditions
Safe	Use is free from any known unacceptable risks, for which the probable benefits of AI use outweigh any probable risks

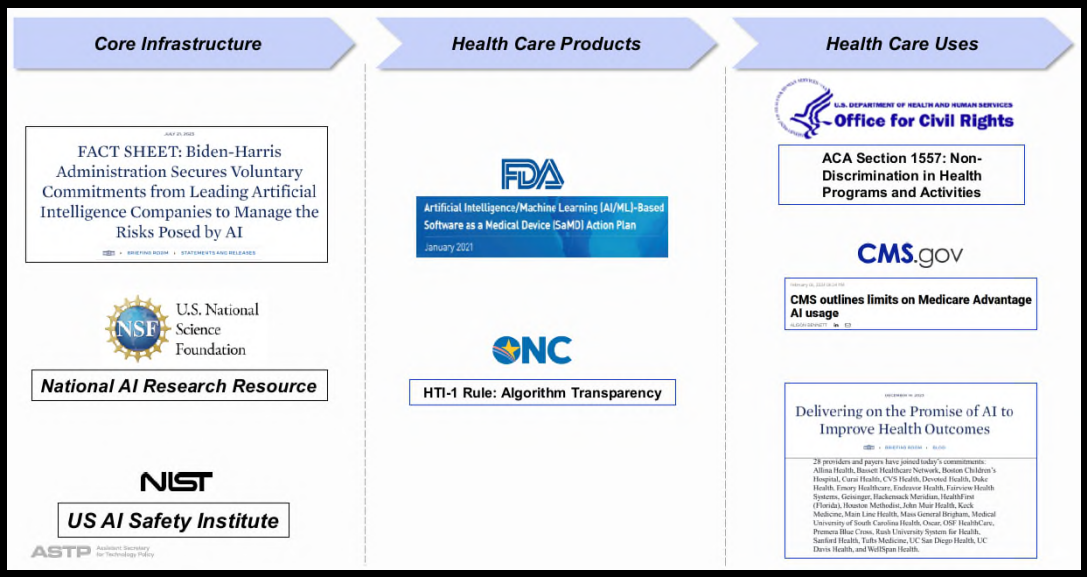
36

HHS AI Strategic Plan



37

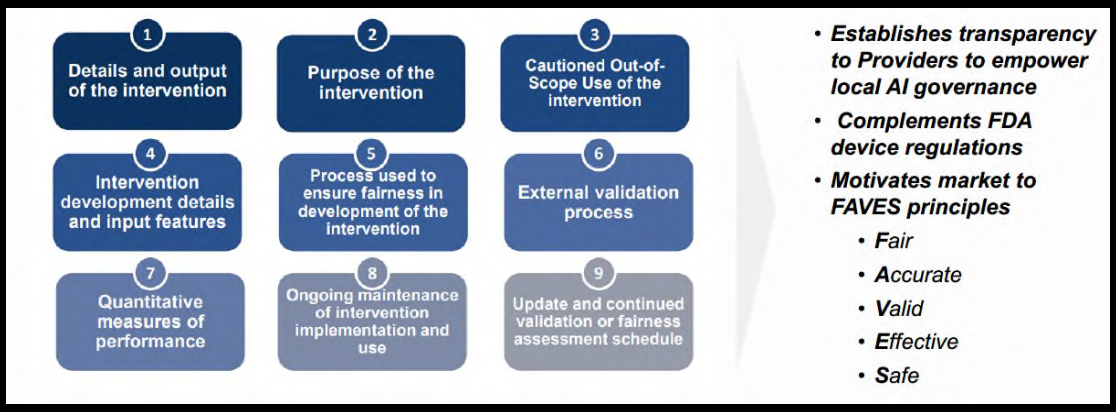
Health AI Regulation and Collaboration



38

Required "Nutrition Label" for AI-based Technologies in EHRs

Required as of January 1, 2025



39

Questions? Thank You!

Contact John: jfhoward@clarkhill.com

40

Section 3 (6:25 – 6:45)

Summary of 2025 Government HC Investigations, Enforcement Actions & Anticipated Priorities for 2026

Presented by: Laura Reilly O'Hara, Member, Healthcare &
Crane Pomerantz, Member, Litigation

clarkhill.com

41

Department of Justice (DOJ) Enforcement Actions

42

42

2024 and 2025 DOJ Enforcement Actions

FY 2024 : DOJ recovered **$2.9B** in False Claims Act settlements, **$1.7 of which was healthcare related.**
Second largest year for recoveries on record, behind only FY 2021, which we can fairly attribute to COVID fraud.

FY 2025: DOJ recovered **$6.8B** in False Claims Act settlements, **$5.7B of which was healthcare related.**

Notably, two large trial verdicts related to the pharmaceutical industry made up more than 44% of the overall healthcare-related recoveries, or approximately $2.5 billion (for $1.6 billion, and over $948 million respectively).

Per a DOJ press release, 1297 qui tam lawsuits were filed in FY 2025, vs. 980 in FY 2024, but because of the length of time these cases take to litigate, a mere increase in the filing of cases wouldn't explain the increase in the number of settlements

43

43

2024 and 2025 Enforcement Actions:

Biggest trial verdicts:

$1.6 billion verdict against a pharmaceutical company (Janssen Products, a Johnson & Johnson unit) — In the case *U.S. ex rel. Penelow v. Janssen Products LP*, a trial jury and court judgment found that the company caused submission of false claims to federal healthcare programs by making false or misleading statements about certain prescription drugs, resulting in a roughly $1.6 billion award (including treble damages and penalties) – off-label marketing of HIV drugs. **UNDER APPEAL** – not a recovery

Roughly $948.8 million judgment against CVS Health's *Omnicare* unit — A federal judge ordered CVS/Omnicare to pay about $948.8 million in penalties and damages after a whistleblower trial found the company fraudulently dispensed drugs without valid prescriptions and billed federal healthcare programs for those claims. – **CVS stated it intends to appeal and its subsidiary Omnicare declared Bankruptcy.**

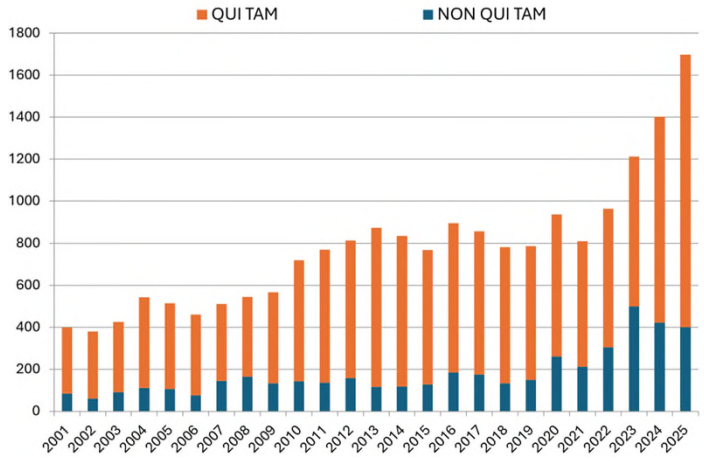
Biggest settlements for FY 2024:

Rite Aid - $408m – No legitimate medical purpose and not issued in the usual course of professional practice
Endo - $475m - used a marketing scheme that targeted healthcare providers that EHSI knew were prescribing Opana ER for non-medically accepted indications.

44

44

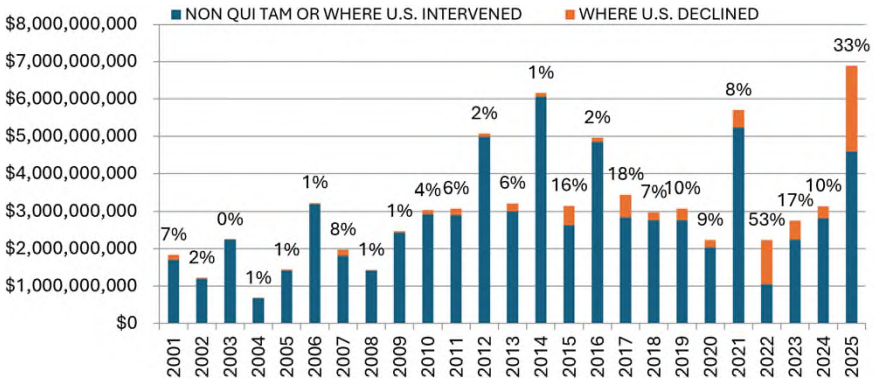
Number of FCA New Matters, Including Qui Tam Actions



Source: DOJ "Fraud Statistics – Overview" (Jan. 16, 2026).

45

Settlements or Judgments in Cases Where the Government Declined Intervention as a Percentage of Total FCA Recoveries



Source: DOJ "Fraud Statistics – Overview" (Jan. 16, 2026).

46

Takeaways and Predictions:

47

47

What To Do If You Receive a CID?

48

48

United States of America ex rel. Cheryl Taylor v. Healthcare Associates of Texas, LLC.

HCAT is a 400 employee value based primary care provider in DFW that was acquired by Optum in 2022.

Background:

Whistleblower lawsuit alleging fraudulent Medicare billing for:

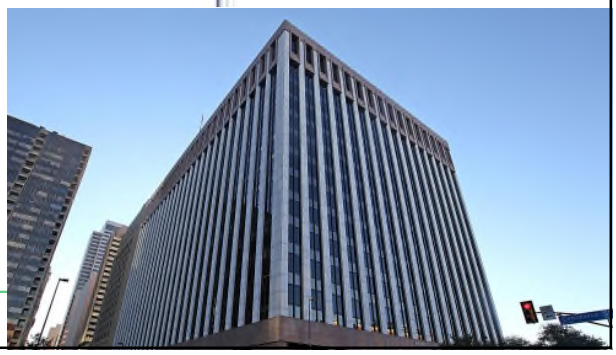
Services performed by uncredentialed or unlicensed providers.

Splitting bills to obscure the identities of treating providers.

Charging Medicare inflated rates for services.

The lawsuit alleged a conspiracy among HCAT entities, its founding physicians, former CEO and ex-Chief Compliance Officer. The jury upheld these claims, finding all defendants liable for the schemes.

The lawsuit alleged a conspiracy among HCAT entities, its founding physicians, former CEO and ex-Chief Compliance Officer. The jury upheld these claims, finding all defendants liable for the schemes.



49

United States of America ex rel. Cheryl Taylor v. Healthcare Associates of Texas, LLC. (cont.)

After a two-week trial, the jury found 21,844 false claims were submitted to Medicare, for a total of **$2,753,641.86** in actual damages.

Under the FCA, the statutory penalty for each false claim ranged from $5,500 to $27,894. The math based on that formula resulted in an awarded civil penalty of **$448,817,000**—over 100 times the actual damages awarded.

The Court substantially reduced the provider's penalties to three times the actual damages, setting total liability at **$16,521,851.16**.

The Court determined that the FCA's mandatory per-claim penalty, when applied in this case, violated the Eighth Amendment's Excessive Fines Clause, which prohibits "grossly disproportional" fines relative to the offense. In evaluating proportionality, the Court considered:

The nature of the violation: The case involved improper Medicare billing based on rules violations as opposed to more egregious conduct such as fictitious claims for services never rendered.

The magnitude of harm: While the government was harmed, the actual damages were quantifiable at $2.75 million, making a $448 million penalty excessively punitive.

The ratio of penalty to damages: The proposed penalty was over 100 times the actual damages, significantly higher than penalties upheld in prior FCA cases, where courts found ratios of 3:1, rather than 8:1, more appropriate.

Takeaways:

Excessive fines clause in the 8th Amendment: Defendants facing outsized FCA penalties should consider raising Eighth Amendment arguments, particularly when statutory fines vastly exceed actual damages. Courts may reduce excessive fines when they result in disproportionate liability.

Government fraud enforcement remains aggressive: Despite this ruling, health care providers should continue prioritizing compliance with Medicare and Medicaid billing regulations.

50

Dinner
15 Minute Break

We will resume programming at 7:00 PM.

clarkhill.com

51

Section 4 (7:00 – 7:20)

From Information Blocking to Sharing: Operationalizing the 21st Century Cures Act in Hospitals & Clinics

Presented by: Paul Schmeltzer, Member, Cybersecurity and Data Privacy

clarkhill.com

52

Agenda

1. What "information blocking" is (and isn't)
2. Risky practices & how to fix them ("share by default, secure by design")
3. Using exceptions the right way (fast, narrow, documented)
4. Oversight readiness: metrics, audits, and proof
5. 30/60/90-day action plan

53

What Counts as Information Blocking?

- Actors: providers, HIN/Es, developers
- Data: EHI in scope (not just labs/notes)
- Activity: practices likely to interfere with access, exchange, or use
- Intent: knowledge/recklessness matters
- Bottom line: default is share, unless a narrow exception applies

54

The “Usual Suspects” (Risky Practices)

- Blanket result holds until physician reviews
- Forcing in-person pickup when portal delivery is feasible
- Over-blocking adolescents or proxies without nuance
- Rejecting patient-selected apps by default
- Slow, manual fax fulfillment when digital is available
- All-or-nothing denials citing “security” without analysis

55

Share by Default, Secure by Design

- **Default release rules:** immediate for most labs/notes/images
- **Role-based** portal access (patient, proxy, adolescent tiers)
- **API pathway:** SMART on FHIR app access with vetting
- **Least-friction channels:** portal/API first, paper last
- **Guardrails:** automated checks + real-time alerts

56

Exceptions—Use Them Right

- **Preventing Harm:** credible risk to life/safety
- **Privacy:** patient preference, law, or consent limits
- **Security:** specific, documented threat; proportionate control
- **Infeasibility:** truly can't do it (not won't)
- **Content & Manner:** offer alternative format/tech now

57

Exception Decision Log

- **Request/Trigger:** who asked, what data, when
- **Exception Invoked:** which one, why it fits
- **Fact Basis:** risk analysis, policy cites, participants
- **Scope & Duration:** what's limited, for how long
- **Alternatives Offered:** content/manner options
- **Outcome & Timestamp:** decision + release/deny time

58

Fixing High-Risks

- **Lab Results:** release immediately; auto-flag only specific sensitive panels for review windows
- **Clinical Notes:** default release; suppress only note types with defined risks (e.g., psychotherapy notes/excluded categories)
- **Third-Party Apps:** publish criteria; auto-approve known safe profiles; document security denials with alternatives

59

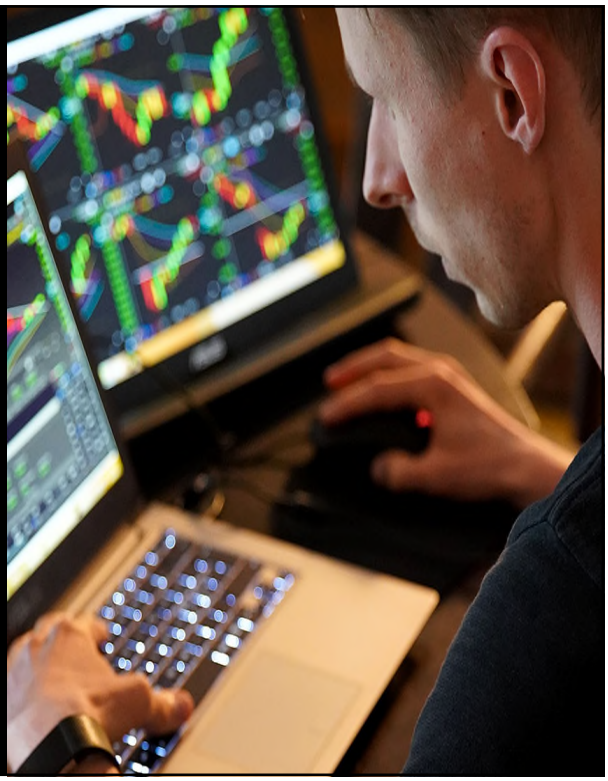
Fees, Format & Fulfillment

- **No "gotcha" fees:** cost-based, reasonable, disclosed
- **Fastest channel first:** portal/API > secure email > paper
- **Content & Manner:** if preferred tech not possible, offer workable alternatives now
- **Turnaround SLAs:** e.g., same-day electronic for routine EHI

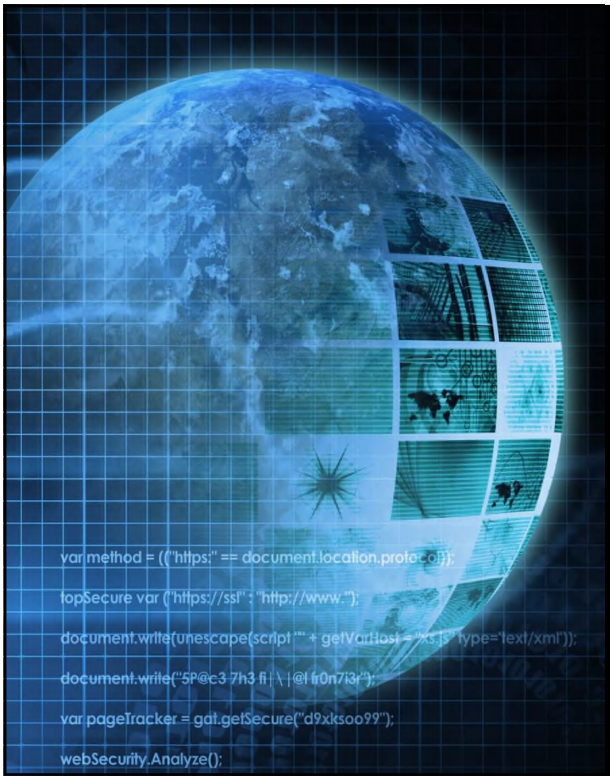
60

Oversight Readiness: Metrics to Track

- Percentage of EHI auto-released without manual touch
- Median time-to-fulfill (portal/API vs. other)
- Exception rate per 1,000 releases (by type)
- Top 5 denial reasons and their corrective actions
- App approvals/denials with timestamps & alternatives



61



Governance & Accountability

- **Policy set:** Release rules, exception SOPs, decision log
- **Committee:** Privacy, Security, CMIO, Nursing, HIM, Legal
- **Training:** frontline scripts + role-based refreshers
- **Audits:** random chart pulls; exception sampling
- **Issue response:** 30-day CAP for outliers

62

Scripts Your Staff Can Use

- **Privacy exception:**

  "We can't share this portion because [specific reason], but we can provide [alternative] today."

- **Security exception:**

  "We can't connect to that app right now due to [specific risk]; here are two secure alternatives we can provide today."

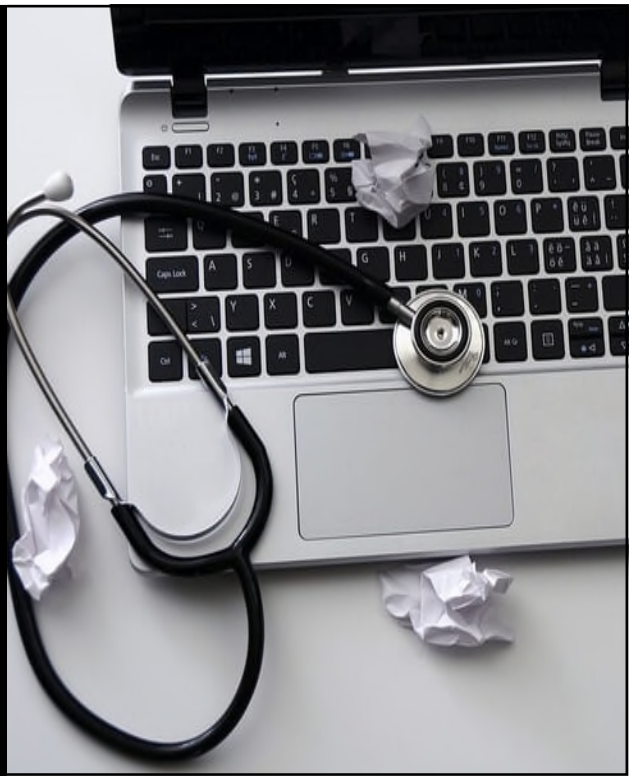
- **Content & manner:**

  "If PDF isn't possible via portal, we can send a direct secure email within 24 hours."

63

Common Pitfalls to Avoid

- Using "provider review" as a **universal delay**
- Calling something "security" without a **threat analysis**
- **All-or-nothing** adolescent/proxy blocks
- Saying "we can't" when you mean "we haven't built it yet"
- Forgetting to **offer alternatives** in real time



64

Case Study

- **Problem:** 72-hour hold on all labs "for courtesy calls"
- **Intervention:** default instant release; hold only for X panels
- **Support:** clinician messaging template + alerting
- **Result:** 94% same-day access; complaints ↓; no safety events

65

Resources & Takeaway

- **Takeaway:** Share by default; exceptions are scalpel, not sledgehammer
- **Resources:** Policies, log template, dashboard metrics
- **Contact:** Paul Schmeltzer | **pschmeltzer@clarkhill.com** or (323) 497-4493

66

Section 5 (7:20 – 7:50)

Healthcare Provider Panel: Texas Non-Compete Law (SB 1318)

Moderated by: James Stafford, Member, Healthcare

Panelists: Sharn Barbarin, MHA, FACHE, Chief Executive Officer at Medical City Healthcare Arlington &
Dr. Valentine Gibson, Anesthesiologist and Chief Development Officer – Meridian Division, National Partners in Healthcare I Chief of Anesthesiology and Obstetrical Anesthesiology – Medical City Arlington

clarkhill.com

67

Today's Panelists

Moderator
James Stafford III
Member, Healthcare Practice Group, Clark Hill PLC

Hospital Leadership Perspective
LaSharndra "Sharn" Barbarin, MHA, FACHE
CEO, Medical City Arlington | Fellow, ACHE

Physician Perspective
Dr. Valentine Gibson, MD
Board-Certified Anesthesiologist | Vice-Chief of Anesthesia, & former Chief of Staff, Medical City Arlington

68

SB 1318: Key Provisions

Duration
1 Year Maximum
(reduced from typical 2-3 year terms)

Geographic
5-Mile Radius
from primary practice location

Scope
Physicians
mid-level providers: open question

Buyout Rights
Preserved
physicians may buy out restrictions

69

Today's Discussion

- Industry adaptation strategies
- Workforce retention alternatives
- Physician mobility & continuity of care
- Practice structure implications
- Mid-level provider considerations
- Finding common ground

70

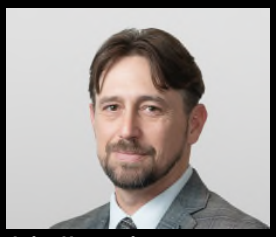
Key Takeaways

1. Review existing physician agreements for compliance
2. Enforcement and interpretation will evolve as courts apply the new law
3. Consider retention strategies beyond non-competes
4. Balance employer protection with physician autonomy

71

Questions?

Tim McGibboney
tmcgibboney@clarkhill.com



John Howard
jhoward@clarkhill.com

Laura Reilly O'Hara
lohara@clarkhill.com

Crane Pomerantz
cpomerantz@clarkhill.com

Paul Schmeltzer
pschmeltzer@clarkhill.com

James Stafford
jstafford@clarkhill.com

72

Thank You

Legal Disclaimer
The views and opinions expressed in this material represent the view of the authors and not necessarily the official view of Clark Hill PLC. Nothing in this presentation constitutes professional legal advice nor is it intended to be a substitute for professional legal advice.

Clark Hill

73