Agentic AI in Healthcare:
Navigating Regulatory Uncertainty and Building Governance That Lasts

Preparing **governance, accountability, and risk frameworks** before regulations fully take shape.

WEEK 2: VIRTUAL SUMMER SERIES
JULY 1 | 12:00 - 1:00 PM CT

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A box.

Resources

Upcoming events, slides & resources linked.

Recording

Recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Clearwater

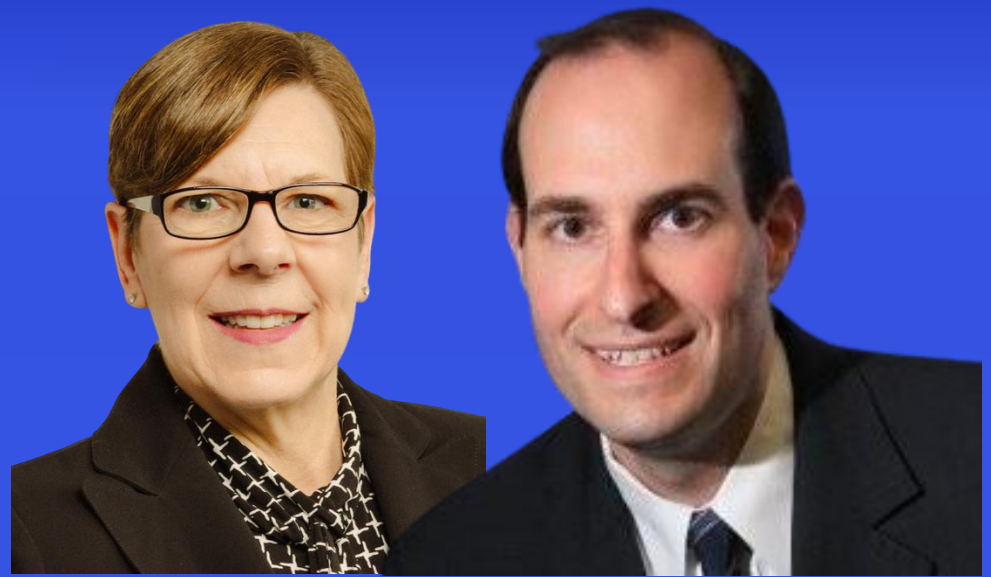
Agenda

- Welcome + Introductions
- Presentation Content: Agentic AI in Healthcare: Navigating Regulatory Uncertainty and Building Governance That Lasts
- Q+A

FEATURING:

Dawn Morgenstern, **Chief Privacy Officer and Senior Principal Consultant, Privacy & Compliance Services**, Clearwater

Adam Greene - **Partner,** Davis Wright Tremaine LLP



What Makes Agentic AI Legally Different

PREDICTIVE AI

- Flags a risk or predicts an outcome
- Human reviews the output
- Accountability: the person who acted on it
- Governance: accuracy & bias testing
- Liability: traditional negligence framework

GENERATIVE AI

- Drafts content in response to a prompt
- Human reviews before use
- Accountability: user who deployed it
- Governance: output quality & safety
- Liability: evolving, generally settled

AGENTIC AI

- Acts — schedules, denies, routes, logs
- Multi-step; reduced human checkpoints
- Accountability: UNSETTLED
- Governance: action accountability, audit trails
- Liability: new territory — courts AND federal agencies defining it now (ARPA-H ADVOCATE)

The shift: from "Did the model answer correctly?" to "Who is accountable when the system acts wrongly?"

Use Cases & Risk: Where to Move, Where to Pause

▲ HIGHER RISK

Prior Authorization Denials
Direct access-to-care impact — Lokken precedent applies

Clinical Documentation & Triage Support
Agent errors compound in downstream clinical decisions

Discharge Planning & Care Coordination
PHI-heavy; multi-system action chains

Inpatient Monitoring & Alerting
ARPA-H ADVOCATE: federal agentic cardiovascular AI agent — adjusts meds, appointments, diet autonomously

Revenue Cycle & Scheduling
Lower patient risk — safer starting point for agentic pilots

▼ LOWER RISK / SAFER STARTING POINT

The federal government is already deploying agentic AI (ARPA-H ADVOCATE). For private organizations, before any workflow goes live

Q1
Who approved this agent's access and scope?

Q2
What does it log at each decision point?

Q3
Who has authority to override or shut it down? (ADVOCATE builds human oversight into its FDA pathway — your commercial deployment should too)

If any answer is "unclear" — the workflow is not ready for production.

State AI Patchwork: Burden & Strategy

Colorado — SB 26-189 (May 2026)
Replaced 2024 AI Act; narrower ADMT notice law effective Jan 1, 2027. DOJ blocked predecessor.

Illinois & Texas (Jan 2026)
AI hiring/employment laws now in effect — algorithmic discrimination obligations.

California (2026 wave)
Multiple agency rules; SB 1047-era proposals still active. Highest regulatory volume.

Federal: No preemption floor
Trump EO 14365 directed DOJ to challenge state AI laws. Landscape may simplify — or fragment further.

How should organizations respond?

⚠ Build to Strictest Rule

- Tracks tightest state standard
- HIGH RISK: Colorado law stayed within weeks of effective date
- Rules may be preempted, revised, or litigated away
- Over-investment in rules that evaporate

✓ Build to Principles

- Anchor: transparency, human review, accountability
- Satisfies any state's substantive intent
- Survives regulatory change and preemption
- Enables compliance with Colorado ADMT, CA, TX, IL — simultaneously

Bottom line: principles outlast any single statute.

Regulatory Landscape: What to Watch Right Now

FDA: NEW PROPOSALS IMMINENT

Watch Now

FDA signals new policy proposals “in weeks and months to come”

- June 2026: FDA’s Abramson signals new proposals “in short order” — risk-proportionate oversight, lifecycle monitoring
- Jan 2025 TPLC draft guidance still in effect: postmarket plans, bias docs required
- ARPA-H ADVOCATE: federal agentic cardiovascular AI agent with FDA authorization pathway built in
- SaMD classification boundary for agentic AI: still UNSETTLED — document as if regulatable
- 1,250+ AI-enabled devices authorized; generative/agentic: zero authorized to date

HIPAA SECURITY RULE NPRM

In Limbo

Published Jan 2025; no final rule as of June 2026

- First substantive update since 2003
- 7,330 comments on HHS clinical AI RFI (Dec 2025); ~4,745 on HIPAA NPRM — intense federal engagement
- $9B projected year-one compliance cost — 100+ orgs sought withdrawal
- Target date May 2026 has passed; timeline unknown
- ONC HTI-5 proposed rule would REMOVE AI transparency requirements from certified EHRs — do not rely on certification alone
- Build to current OCR enforcement expectations — not the NPRM

WHERE ENFORCEMENT HITS FIRST

Litigation

Private plaintiffs move first; federal agencies accelerating

- Lokken v. UHG (D. Minn.): 90% AI error rate alleged; broad discovery ordered Mar 2026
- OCR Phase 3 audits underway — 50 entities; top gap: risk analysis
- OCR, FTC, state AGs can apply existing law NOW
- No agentic-specific rule required for enforcement action
- CMS CRUSH initiative: AI-powered fraud detection now active; CMS also seeking AI for Medicare plan selection
- 4 states (AZ, IL, NH, VA) have introduced AI sandbox/regulatory relief bills in 2026 — potential compliance pathway
- Gap closing faster than agentic-specific rules are forming

Governance That Lasts

1

Anchor to NIST AI RMF — not to any single rule

Build to Govern-Map-Measure-Manage + AI 600-1. NIST survives any state preemption or federal rule change. Look to HHS's OneHHS model: risk-tier AI by impact, maintain a use-case inventory, apply minimum risk controls to high-impact systems by deadline. The question that anchors it all: who is accountable when the system acts?

2

Vendor contracts must address agentic AI before deployment

Most BAAs predate agentic AI. Require: decision logs with access rights • model change notification • bias testing documentation • explicit audit rights. Warning: ONC's HTI-5 proposed rule would remove AI transparency requirements from certified EHRs — don't rely on certification alone. Colorado SB 26-189 voids clauses that shift AI discrimination liability to vendors.

3

"Human-in-the-loop" needs structure, not just a policy statement

Meaningful oversight = named override authority + documented escalation triggers + pre-action audit trails. ACL Deputy Administrator Cronin on federal agentic AI: "We want to supplement, not replace human connection." That's your HITL standard. McKinsey 2026: "The scariest failures are the ones that cannot be reconstructed because the workflow wasn't logged."

Be Defensible Before You Deploy

Documentation to have in place before any agentic AI goes live:

- ✓ **AI Inventory Entry**
  Scope, access level, named owner
- ✓ **Risk Tier Classification**
  Follow HHS OneHHS model: high-impact AI must have risk controls by design
- ✓ **Logging Architecture**
  What is captured, where, by whom
- ✓ **Escalation Protocol**
  Named authority; documented triggers
- ✓ **Vendor Agreement**
  Audit rights, change notification, bias testing
- ✓ **Patient-Facing Disclosure**
  Where required by state or expected by OCR

THE GUIDING PRINCIPLE

Govern the action, not just the output.

ARPA-H ADVOCATE shows the standard: transparency, human oversight, and FDA pathway built in from day one.

For your organization: Who is accountable when the system acts wrongly?

Name the owner. Log the decision. Define the override.

Q&A

Clearwater

Healthcare's Cyber Briefing

CRITICAL THREAT BRIEF FOLLOWED BY

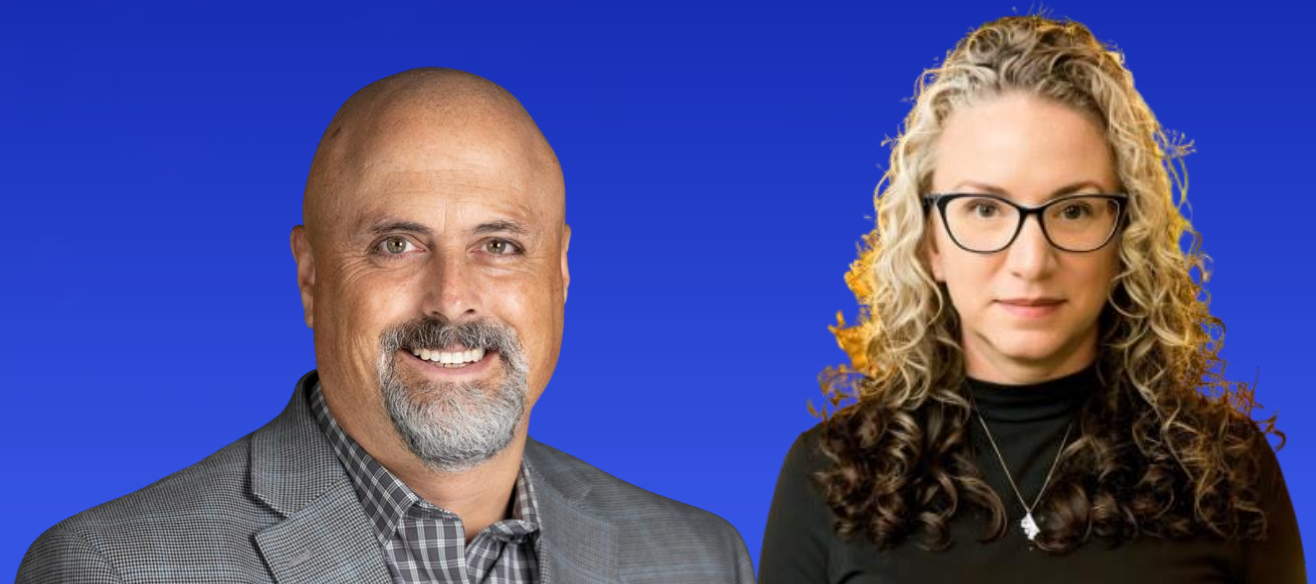
RECOVERY UNDER PRESSURE: WHAT SEPARATES WEEKS FROM MONTHS IN HEALTHCARE INCIDENT RESPONSE

JULY 9 @ 12PM CT!

FEATURING:

David Bailey, VP of Consulting Solutions & Strategy

Heather Hanson, Manager, Resiliency Services



Coming Next

When the Attackers Bring AI:
2026 Healthcare Threats in Plain View

WEEK 3: VIRTUAL SUMMER SERIES
JULY 8 | 12:00 - 1:00 PM CT

From Commitment to Execution:
Operationalizing AI Governance in Healthcare

WEEK 4: VIRTUAL SUMMER SERIES
JULY 15 | 12:00 - 1:00 PM CT

State of AI in Healthcare:
Where the Industry Actually Is

WEEK 5: VIRTUAL SUMMER SERIES
JULY 22 | 12:00 - 1:00 PM CT

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Clearwater

Healthcare–Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.