Scalable Technology-Enabled Auditing & Monitoring for Health Care Compliance

Molly VandeVoort, JD, MPH

August 2026

Disclaimer and AI Disclosure

This presentation is designed to provide general information on pertinent legal topics. The information is provided for educational purposes only. Statements made or information included do not constitute legal or financial advice, nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the author.

This information contained in this presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. Substantive changes in the law subsequent to the date of this presentation might affect the analysis or commentary. Similarly, the analysis may differ depending on the jurisdiction or circumstances. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.

This presentation was developed with the assistance of generative AI tools. AI was used to support restructuring and outlining, visual design, and verifying current authorities. All legal authorities, factual statements, and citations were reviewed and verified by the speaker against primary sources. **All analysis, conclusions, and final content are the speaker's own, and the speaker is responsible for the final work product.**

Presenter

Molly VandeVoort, JD, MPH
Associate
Holland & Hart LLP

Connect on LinkedIn

Acknowledgment. This program builds on a session originally co-developed and co-presented with Adrienne Chase, Area Chief Compliance Officer, Trinity Health.

Molly advises healthcare providers, payors, and other organizations on regulatory, compliance, and transactional matters. Before entering private practice, she built over 15 years of experience across clinical research, epidemiology, managed care, healthcare operations, and federal healthcare programs, including data modernization and regulatory implementation work tied to complex commercial insurance and Medicaid programs.

Her practice focuses on translating complex healthcare laws into practical operational strategy, connecting legal, clinical, operational, and technical perspectives.

From Point of Use to Program Level

WHERE THIS SESSION FITS

OUR JUNE SESSION

AI Chatbots & HIPAA

The point-of-use decisions providers face when they put an AI tool in front of protected health information.

THIS SESSION

The Program, Zoomed Out

The legal risks and regulatory expectations shaping your auditing and monitoring program as a whole.

THE THROUGH LINE Each step raises its own legal question once monitoring runs on data, not spreadsheets.

MONITORING	RECORD	FLAG	ANALYTICS	ACTION
Scope & vendors	Retention & privilege	Documenting findings	Regulators run it too	Escalation & counsel

Learning Objectives

AFTER THIS SESSION, YOU'LL BE BETTER POSITIONED TO

1. Spot the legal issues in how compliance data and monitoring records get created, retained, and produced.
2. Recognize the contracting and diligence questions worth raising with monitoring and analytics vendors.
3. Judge whether your program is finding its own outliers before the regulators' models do.
4. Identify where attorney-client privilege and work product may be at risk as monitoring automates.
5. Know when a routine finding warrants a call to counsel — and what the first legal steps look like.

Roadmap

A BRIEF FOUNDATION, THEN FIVE LEGAL THEMES

F **Foundation**
Where auditing & monitoring fit, and how regulators judge the system

1 **Regulators' Analytics**
Why enforcement is now data-driven, and what that means

2 **Structuring Data & Records**
Building monitoring records that withstand scrutiny

3 **Vendors & Contracting**
Diligence and contract terms for analytics vendors

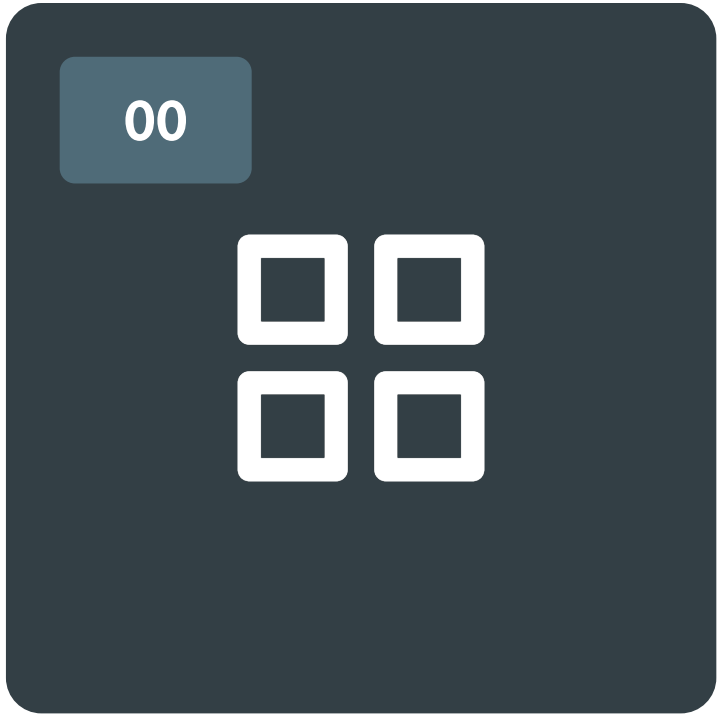
4 **Privilege**
Protecting attorney-client privilege as monitoring automates

5 **From Finding to Investigation**
The legal steps when a routine finding stops being routine

Where Auditing & Monitoring Fit

FOUNDATION.

A quick orientation before the legal themes: the seven elements, the difference between an audit and monitoring, and the system regulators expect to see.



Audit vs. Monitor: The Label Is a Promise

TWO TERMS OF ART WITH DIFFERENT LEGAL CONSEQUENCES

AUDITING

A point-in-time, retrospective examination against a defined standard.

- Independent, objective review
- Defined sample, universe, and test period
- Measured against a statute, regulation, or policy
- Ends in a formal report with recommendations

MONITORING

An ongoing, operational check that runs as the work happens.

- Continuous or recurring cadence
- Owned by compliance or the business area
- KPIs, thresholds, and dashboards
- Feeds escalation and trend reporting

Why the label matters legally. Call it an audit and you promise independence and methodology. Call it monitoring and you promise continuity. Whatever you call it, anchor it to a policy with a defined scope, and write it down. Mislabeling creates expectations, and exposure, you cannot meet.

See OIG General Compliance Program Guidance 15-17 (Nov. 2023) (effective monitoring and auditing).

How Far You Can Actually Scale

FOUR LEVELS OF MATURITY. KNOW WHICH ONE YOU ARE BUILDING FROM

1

SPREADSHEET
level one

Workplan and findings live in Excel. Defensible if scope, criteria, and owner are written down.

risk: it goes stale quietly

2

STRUCTURED RECORDS
level two

Defined fields and allowed values. One record per activity, queryable across sites and years.

risk: nobody owns the schema

3

AUTOMATED MONITORING
level three

Scheduled screens and alerts on live data. Vendor terms and privilege design become controls.

risk: privilege gets harder

4

ANALYTICS PROGRAM
level four

Peer and outlier modeling turned inward, governed and documented as Element 5.

risk: a model you never validated

Know your level before you buy. Every recommendation that follows lands differently at level one than at level four.

See OIG General Compliance Program Guidance 57 (Nov. 2023); DOJ Evaluation of Corporate Compliance Programs (updated Sept. 2024).

What OIG & DOJ Expect

AN EFFECTIVE, DEFENSIBLE SYSTEM, NOT ISOLATED AUDITS

PREVENT
Stop violations before they occur

DETECT
Find issues through monitoring & auditing

CORRECT
Remediate and enforce accountability

The governing guidance

- **OIG General Compliance Program Guidance.** *November 2023*
- **OIG Industry Segment-Specific Guidance.** *first ICPG: nursing facilities, Nov 2024*
- **DOJ Evaluation of Corporate Compliance Programs.** *updated 2024*
- **OIG Work Plan and Federal Sentencing Guidelines.** *ongoing*

OIG, General Compliance Program Guidance (Nov. 2023), https://oig.hhs.gov/documents/compliance-guidance/1135/HHS-OIG-GCPG-2023.pdf; DOJ, Crim. Div., Evaluation of Corporate Compliance Programs (updated Sept. 2024), https://www.justice.gov/criminal/criminal-fraud/page/file/937501/download.

One Obligation, Four Realities

WHERE YOU SIT DETERMINES WHAT YOU CAN SEE, AND WHO COMES LOOKING

1. **Pharmacy** You are usually the one being audited. The board of pharmacy, the DEA, 340B integrity reviews, and PBM audits all run on data you do not control.

2. **PBM** You audit others, at scale. Your findings get challenged, so your methodology has to survive being read by opposing counsel.

3. **Regional hospital** One or two people and a spreadsheet, covering billing, coding, and physician arrangements. The constraint is capacity, not ambition.

4. **Multi-state system** Fifty sets of rules at once. Peer review privilege, state Medicaid fraud unit analytics, and the question of which entity holds the privilege.

The through line. The Element 5 obligation is identical for all four. What differs is the data you can reach, and the regulator who reaches you first.

Working With AI: Lead, Team, or Delegate

DECIDE THIS BEFORE YOU BUILD: HOW MUCH OF THE WORK THE MACHINE DOES

LEAD
human only

You do the work; no AI. Privileged matters, judgment calls, final conclusions.

e.g., interviewing staff, signing the report

TEAM
human + AI together

AI drafts, summarizes, and checks in real time while you steer every step.

e.g., co-drafting an audit scope

DELEGATE
AI first, you verify

Hand AI a bounded, verifiable task; review the output before you rely on it.

e.g., building a timeline from records

This choice runs through every theme that follows — the record you can defend, the vendor you rely on, and the privilege you can still claim.

See DOJ Evaluation of Corporate Compliance Programs (updated Sept. 2024) (AI governance and risk management as compliance-program elements).

Regulators Are Using Analytics Too

THEME ONE.

Enforcement is now data-driven. OIG builds its own models to find outlier providers, which changes the calculus for getting ahead of your own risk areas.

OIG's Data-Driven Enforcement

OUTLIER ANALYSIS AS FRONT-END DETECTION: DATA → AUDIT FINDING → AFFIRMATIVE LITIGATION

$33M+
recovered across these actions

100+
settlements and CMPs

6
high-risk billing areas modeled

Data-driven enforcement example	Outcome (as reported)
Operation Wheel and Deal (ambulance to inappropriate destinations)	24+ CMP settlements, more than $4M recovered
Epidural steroid injections	4 settlements, more than $1M
Facet joint injections	6 settlements, about $1.8M
Double-payment ambulance	26 settlements + 2 exclusions, more than $12M
Urine drug testing (Modifier-59 modeling)	11 CMP + 1 FCA settlement, more than $14M
Molecular pathology (HCPCS G0452)	29 physician settlements, more than $870K

G. Hymans, Deputy Branch Chief, Exclusions Branch, HHS-OIG Office of Counsel, "OIG Use of Data," HCCA Data & Analytics Meeting (Mar. 2026).

Enforcement Runs on Fused Data

WHAT CHANGED SINCE MARCH: DOJ'S 2026 NATIONAL HEALTH CARE FRAUD TAKEDOWN

455
defendants charged in June 2026

$6.5B
in alleged false claims

$10B
caught and suspended before payout

What is new in 2026	Why it matters to your program
Data Fusion Center | Financial Intelligence Review Team	Claims, financial and law enforcement data in one view; one 2026 case opened within five days of review
National Fraud Enforcement Division	A single DOJ hub for federal benefit program fraud
FOCUS initiative | Civil Division, Apr. 30, 2026	DOJ is prioritizing outside data miners who build fraud signals from public data and file them as qui tam relators
CMS administrative action	1,079 providers suspended; 1,403 revocations
HHS-OIG action	1,400+ exclusions; 48 CMP settlements
Parallel consequences	Criminal, civil, administrative, and licensure at once

DOJ, National Health Care Fraud Takedown (June 23, 2026); DOJ Civil Div., Press Release 26-423, "Civil Division Announces FOCUS Initiative for Data Miners Filing Qui Tam Complaints" (Apr. 30, 2026); DOJ Health Care Fraud Unit, Data Fusion Center.

⚠ WISeR: AI Now Reviews Your Claims

CMS INNOVATION CENTER MODEL, LIVE SINCE JANUARY 1, 2026 IN SIX STATES

What it is. A CMMI model in which technology companies, not providers, are the participants, using AI and machine learning to make prior authorization and pre-payment medical review determinations in Original Medicare.

Service on the list

Selected Original Medicare items and services in AZ, NJ, OH, OK, TX, and WA

Two pathways

Prior authorization by the model participant, or post-service pre-payment review

AI-assisted determination

Human clinicians must review any non-affirmation before it issues; an exemption program is coming

The government is auditing with AI too: the model-transparency questions you ask your vendors now run in both directions.

CMS Innovation Center, WISeR Model, Provider and Supplier Operational Guide v7.0 (July 30, 2026); implemented Jan. 1, 2026 in AZ, NJ, OH, OK, TX and WA. Senate rejected the motion to proceed to S.J. Res. 198 (CRA disapproval), 46-50, Roll Call Vote 199 (July 16, 2026).

The Work Plan Is a Dataset

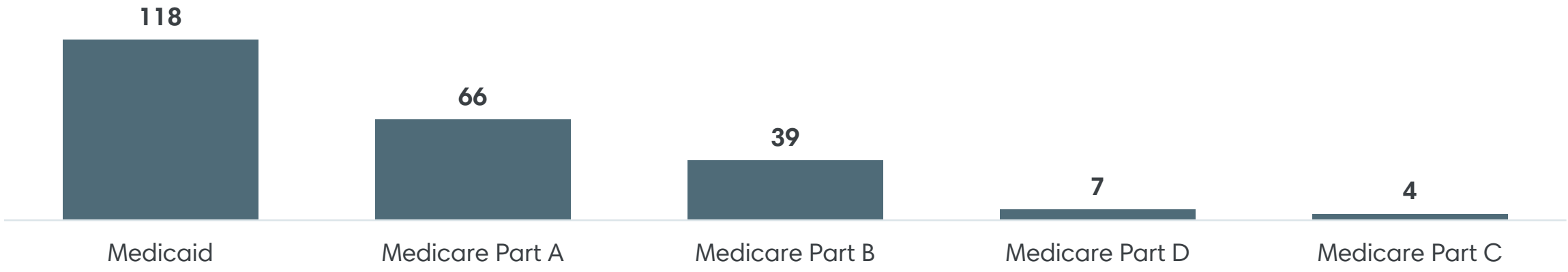
ALL 444 HHS-OIG WORK PLAN ITEMS, PULLED AUGUST 12, 2026

209
active OIG projects today

118
target Medicaid, vs. 105 Medicare

39%
have no public title yet

Active OIG Work Plan items by program



HHS-OIG Work Plan, export of Aug. 12, 2026: 444 items, 209 active. Chart shows active items by financial group tag; items may carry more than one tag.

The Stakes: Find Your Outliers First

YOUR ANALYTICS PROGRAM IS ELEMENT 5 IN ACTION

The real question is simple: are you finding your own outliers, or waiting for OIG's models to find them first?

WHAT TO DO ABOUT IT

- **Run peer and outlier analysis on your own high-risk billing areas**
  Mirror the methods enforcement uses: the same modeling, turned inward.
- **Prioritize the areas OIG is visibly modeling**
  Injections, drug testing, pathology, ambulance, and current Work Plan items.
- **Treat analytics as compliance work, not an IT side project**
  Document it as Element 5, with scope, criteria, and follow-through.

See OIG General Compliance Program Guidance (Nov. 2023) (data-driven risk detection); DOJ Evaluation of Corporate Compliance Programs (updated Sept. 2024).

Structuring Data & Records to Withstand Scrutiny

THEME TWO.

How you structure compliance data and monitoring records determines whether they can be reported, trended, and defended when a regulator asks to see them.

Documentation Is Defensibility

IF IT IS NOT WRITTEN DOWN, THE GOVERNMENT TREATS IT AS IF IT DID NOT HAPPEN

1

The copy-paste plan

Legal exposure: Proves you did not use your own risk assessment.

2

Undocumented method

Legal exposure: No written record: treated as if it never happened.

3

Findings go nowhere

Legal exposure: Repeat findings become exhibit A in an aggravated case.

4

Reporting in a vacuum

Legal exposure: Leadership cannot govern what it cannot see.

Cf. United States v. Balance Diagnostics USA, LLC, No. 15 Civ. 2641 (VSB) (S.D.N.Y. 2024) (settlement; no meaningful FMV analysis for provider subleases).

Anatomy of a Defensible Activity

A STRANGER SHOULD BE ABLE TO PICK UP THE FILE AND SEE EXACTLY WHAT YOU DID AND WHY

WHAT THE RECORD MUST CONTAIN

- Defined scope and population
- Measurement criteria: statute, regulation, policy, or standard
- Sampling method and size, with written rationale
- Named owner, performers, and collaborators
- Contemporaneous working papers

THE ORDER MATTERS

1. **Write purpose and scope** before touching data
2. **Lock the measurement criteria** up front
3. **Choose the sample** and document why
4. **Keep working papers** as you go, not after

Pull data first and you unconsciously fit scope to what the data shows. That is how an audit loses credibility.

See OIG General Compliance Program Guidance 15-17 (Nov. 2023) (documented scope, methodology, and ownership).

Structure the Records: Design the Schema First

IF IT CAN BE QUERIED, IT CAN BE REPORTED, TRENDED, AND DEFENDED

AD HOC SPREADSHEET FIRST

- Repeated columns across many sheets
- Sparse fields and nulls everywhere
- No link between current and future plans
- Cannot query across plan types
- Painful migration when systems unify

SCHEMA-FIRST DESIGN

- Normalized records with clear relationships
- No duplication or sparse columns
- Keys enforce consistency
- One system for current and future plans
- Plugs into GRC tools without rework

The regulator's test. When OIG says "show me your monitoring plan and prove you executed it," a queryable record answers in minutes. A plan you can only scroll will go stale, and garbage structure means garbage analytics later. Define the fields and their allowed values before you build.

See OIG General Compliance Program Guidance 55-67 (Nov. 2023) (effective monitoring and auditing; data-driven risk detection).

Five Questions a Regulator Will Ask

THE DOCUMENTATION LENS FROM OIG GCPG AND THE DOJ ECCP

1. **Is it risk-based?** The plan traces back to your enterprise risk assessment.
2. **Is it documented?** Written scope, methodology, ownership, and frequency for every activity.
3. **Do findings go somewhere?** Corrective action plans with owners, deadlines, and validation.
4. **Does leadership see it?** Committee minutes, board reports, dashboards.
5. **Does it evolve?** The plan pivots as risks emerge and feeds next year's assessment.

OIG General Compliance Program Guidance (Nov. 2023); DOJ Evaluation of Corporate Compliance Programs (updated Sept. 2024).

Contracting & Diligence With Analytics Vendors

THEME THREE.

As monitoring shifts to outside platforms and analytics vendors, the diligence and contract terms become a core compliance control, not just a procurement formality.

Build vs. Buy: The Legal Lens

FOUR LAYERS OF THE STACK, THREE WAYS TO ACQUIRE THEM

1. **Data foundation.** One schema, one source of truth
2. **Automation.** Scheduled screens, feeds, and alerts
3. **Analytics & dashboards.** KPIs, KRIs, and trend lines
4. **AI capabilities.** Drafting, triage, horizon scanning

BUILD VS. BUY

- **Spreadsheets.** easy to start, brutal to maintain
- **Databases.** scale, but need IT partnership
- **Vendor tools.** check roadmap, data rights, and exit terms

Whatever you choose, you still own the schema, and you still own the risk.

See DOJ Evaluation of Corporate Compliance Programs 8–10 (updated Sept. 2024) (data analytics and automated monitoring capabilities).

Vendor Diligence & Contracting Checklist

THE TERMS THAT PROTECT YOU WHEN THE MONITORING LIVES ON SOMEONE ELSE'S PLATFORM

✓ **Business Associate Agreement**
compliant BAA before any PHI flows

✓ **Data ownership & portability**
you own the data and the outputs

✓ **Permitted use**
no secondary use or model training on your PHI

✓ **Security & subcontractors**
safeguards, breach timelines, flow-down

✓ **Model transparency & change control**
notice of model changes; versioning

✓ **Audit & cooperation rights**
audit, government inquiry, IRO, e-discovery

✓ **Service levels & continuity**
uptime and business continuity

✓ **Exit & records retention**
return or certified destruction of data

Why it bites. When FMV or documentation is thin, regulators infer intent under the Anti-Kickback Statute: DaVita ($34M), Balance Diagnostics ($2.5M), and Dunes ($12.7M) all turned on the absence of a defensible record.

42 U.S.C. § 1320a-7b(b); 42 C.F.R. § 1001.952(d) (compensation set in advance, consistent with fair market value, not by volume or value of referrals).

Monitor the Rules, Not the Claims

STATE REGULATORY CHANGE IS A MONITORING ACTIVITY, AND IT SCALES THE SAME WAY

1 Watch the right sources

Scope: Legislatures and agency rulemaking, insurance and pharmacy board bulletins, Medicaid provider notices, and licensure filings in every state you operate.

2 Triage what it touches

Test: Does the change move a control, a contract term, a disclosure, or a reporting deadline? Most changes need no action - write down that you decided so.

3 Assign an owner and a date

Record: One named owner, one due date, one implementation record. The change is not closed when counsel reads it. It is closed when the control changes.

4 Alert on the fix, not the memo

Control: Build the dashboard that fires if the new requirement still is not being met ninety days later. Tracking awareness is not tracking compliance.

Rutledge v. Pharmaceutical Care Management Ass'n, 141 S. Ct. 474 (2020) (unanimous) (Arkansas Act 900, regulating PBM reimbursement rates, is not pre-empted by ERISA).

Protecting Privilege as Monitoring Automates

THEME FOUR.

Privilege is earned through how a process is run, not applied by stamping a footer. Automation makes routine monitoring look even more like ordinary business, which makes privilege harder to claim, not easier.

Privilege Is Earned, Not Labeled

COURTS LOOK PAST THE FOOTER TO THE SUBSTANCE AND PURPOSE OF THE COMMUNICATION

TO HOLD UNDER SCRUTINY, IT MUST BE

- Made in confidence
- For the primary purpose of legal advice
- Treated as confidential throughout

Stamping "Attorney-Client Privileged" on a routine audit does not create privilege, even if counsel is copied.

COURTS REJECT PRIVILEGE WHEN

- The audit was required as ordinary course
- Same scope and method regardless of litigation
- The report is shared broadly with non-legal staff
- The primary purpose was operational, not legal

Upjohn Co. v. United States, 449 U.S. 383 (1981); In re Kellogg Brown & Root, 756 F.3d 754 (D.C. Cir. 2014); Fed. R. Civ. P. 26(b)(3); Fed. R. Evid. 502; ABA Model Rules 1.6 & 1.13.

Guardrails as Monitoring Automates

SEPARATE THE ROUTINE FROM THE PRIVILEGED, BY DESIGN

The automation problem. Continuous, automated monitoring is the clearest possible example of "ordinary course of business," the exact fact courts cite to deny privilege. The more you automate, the more deliberate your privilege design must be.

1. **Reserve privilege for genuine investigations**
   not routine work product
2. **Counsel directs and controls**
   not merely receives a copy
3. **Segregate the documents**
   never one combined file
4. **Limit distribution; mark consistently**
   need-to-know only
5. **Document the elevation point**
   when routine became counsel-directed
6. **Do not rely on the label**
   a court can order production

Upjohn Co. v. United States, 449 U.S. 383 (1981); In re Kellogg Brown & Root, Inc., 756 F.3d 754 (D.C. Cir. 2014).

When a Routine Finding Turns Into an Investigation

THEME FIVE.

The single most important moment in a monitoring program is recognizing when a routine finding stops being routine, and moving deliberately in the right order.

⚠ Recognize the Turn, Then Move in Order

CHANGE FOOTING DELIBERATELY, NOT ACCIDENTALLY

ESCALATION TRIGGERS

- Signs of intentional misconduct or fraud
- Potential systemic overpayment, not isolated error
- Possible criminal, licensure, or media exposure
- Whistleblower or government inquiry on the same facts

THE FIRST FIVE MOVES

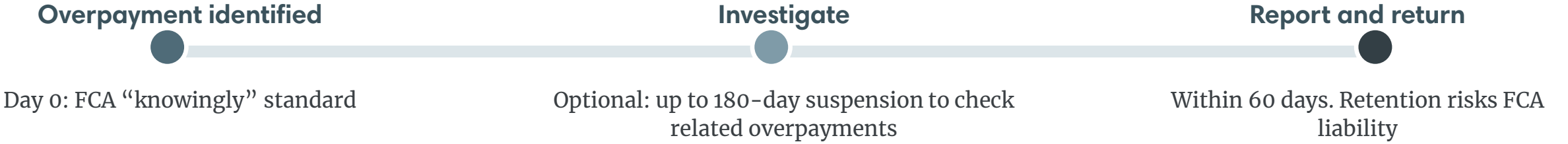
1. Pause the routine audit workflow
2. Engage counsel: privilege by design, not by accident
3. Issue preservation notices; stop auto-deletion
4. Quantify exposure with counsel; scope the lookback
5. Report up, and evaluate self-disclosure (OIG SDP / CMS SRDP)

42 U.S.C. § 1320a-7k(d); OIG Provider Self-Disclosure Protocol; CMS Self-Referral Disclosure Protocol.

⚠ The 60-Day Clock Just Got Sharper

CY2025 MEDICARE PFS FINAL RULE, EFFECTIVE JANUARY 1, 2025

What changed. "Identified" now uses the False Claims Act "knowingly" standard (actual knowledge, reckless disregard, or deliberate ignorance), replacing the older "reasonable diligence" standard.



A monitoring finding can start this clock: escalation is a deadline decision.

ACA § 6402; 42 U.S.C. § 1320a-7k(d); 42 C.F.R. §§ 401.301 to 401.305 (Parts A/B), § 422.326 (Part C), § 423.360 (Part D); CY2025 Medicare Physician Fee Schedule Final Rule, effective Jan. 1, 2025.

⚠ Write It Down: A Sample Escalation Policy

DECIDE WHAT THE BAD DAY LOOKS LIKE BEFORE IT ARRIVES

POLICY SECTIONS

- Purpose & scope
- Definitions: audit, monitoring, investigation
- Annual plan governance & approval
- Activity standards, including AI use
- Reporting & corrective action
- Escalation to investigation
- Record retention & privilege

§ 6 ESCALATION: TEMPLATE LANGUAGE

*If facts suggest potential fraud, intentional misconduct, or systemic overpayment, the reviewer **shall** —*

1. Suspend the activity; cease further staff communications
2. Notify the Compliance Officer within one business day
3. Compliance Officer, with counsel, decides whether it proceeds under privilege
4. Issue preservation notices to all relevant custodians
5. Quantify any overpayment; resolve under the 60-day rule

42 U.S.C. § 1320a-7k(d); 42 C.F.R. §§ 401.301 to 401.305; OIG Provider Self-Disclosure Protocol.

If Prevention Fails: Life Under a CIA

A DOCUMENTED, RISK-BASED PROGRAM IS YOUR INSURANCE POLICY

WHAT A CIA REQUIRES

- Compliance officer & committee obligations
- Board-level certifications
- Independent Review Organization (IRO)
- Annual report to OIG
- Typically a five-year term
- Breach: stipulated penalties or exclusion

WHAT IS NEW IN RECENT CIAs

- Generative AI use disclosed in the Annual Report
- Accuracy certified; same duty on the IRO
- Root cause required in Reportable Event reports
- Expert reports in the first and fourth periods
- Board retains a Compliance Expert within 90 days
- CO cannot lead or report to legal or finance

YOUR INSURANCE POLICY

- Weighed in your favor before penalties
- Under a CIA, the IRO grades your A&M plan
- This deck maps to CIA obligations
- Strong monitoring + timely self-disclosure can avoid a CIA entirely

The cheapest Corporate Integrity Agreement is the one you never have to sign.

42 U.S.C. § 1320a-7; see, e.g., OIG CIAs with EyePoint Inc. (July 2026) and Family Health Care Associates LLC (June 2026) (generative AI disclosure and accuracy certification).

Key Takeaways

FIVE THINGS TO DO MONDAY MORNING

1. **Structure before you collect.** Define the record and its fields first; a queryable plan is a defensible plan.
2. **Put your controls in the contract.** Diligence your analytics vendors; own your data, uses, and exit.
3. **Turn the analytics inward.** Find your outliers before OIG's models do.
4. **Design for privilege.** Segregate routine monitoring from counsel-directed investigation and document the turn.
5. **Write the escalation policy.** Decide the first five moves, and track the 60-day clock, before the bad day.

Score Your Own Program

TEN QUESTIONS. ANSWER THEM HONESTLY BEFORE SOMEONE ELSE ASKS.

01 Can you produce the plan and prove you executed it?

02 Does every activity have scope, criteria, and owner?

03 Can your records be queried across sites and years?

04 Does the plan trace to your current risk assessment?

05 Do findings have owners, deadlines, and closure?

06 Do you run outlier analysis on high-risk billing?

07 Do you know what OIG is working on in your lines?

08 Does your vendor contract cover data and exit?

09 Is routine monitoring separated from privilege?

10 Does your escalation path track the 60-day clock?

Fewer than eight yeses is not a failing grade. It is next year's workplan. Start with the questions you hesitated on and put a date next to each one.

Questions map to OIG General Compliance Program Guidance (Nov. 2023) and DOJ Evaluation of Corporate Compliance Programs (updated Sept. 2024).

Thank You

Running a program? Toolkit tips included at the end of this slide deck.

Advising a program? Happy to compare notes, or co-present this for your client teams.

Molly VandeVoort, JD, MPH | msvandevoort@hollandhart.com
T: (208) 383-3964 | M: (720) 626-2397

Connect on LinkedIn

Selected Authorities & Sources

GUIDANCE

- OIG, General Compliance Program Guidance (Nov. 2023).
- DOJ, Crim. Div., Evaluation of Corporate Compliance Programs (updated Sept. 2024).

STATUTES & REGULATIONS

- Anti-Kickback Statute, 42 U.S.C. § 1320a-7b(b); safe harbors, 42 C.F.R. § 1001.952.
- Physician Self-Referral (Stark), 42 U.S.C. § 1395nn; 42 C.F.R. §§ 411.351 to 411.357.
- False Claims Act, 31 U.S.C. § 3729.
- Civil Monetary Penalties and Exclusion, 42 U.S.C. §§ 1320a-7a, 1320a-7.
- Overpayment (60-day) rule, 42 U.S.C. § 1320a-7k(d); 42 C.F.R. §§ 401.301 to 401.305; 2025 Medicare PFS Final Rule, CMS-1807-F and CMS-4201-F5.

CASES

- Upjohn Co. v. United States, 449 U.S. 383 (1981).
- In re Kellogg Brown & Root, Inc., 756 F.3d 754 (D.C. Cir. 2014).
- Rutledge v. PCMA, 141 S. Ct. 474 (2020).
- United States ex rel. Kogod v. DaVita Inc. (D. Colo. 2024).
- United States v. Balance Diagnostics USA, LLC (S.D.N.Y. 2024).
- Dunes Surgical Hosp., OIG Self-Disclosure Resolution (2024).
- United States ex rel. Carter v. Emergency Staffing Sols., Inc., 2025 U.S. Dist. LEXIS 16579 (2025).

RULES & PROTOCOLS

- Fed. R. Civ. P. 26(b)(3); Fed. R. Evid. 502; ABA Model Rules 1.6, 1.13.
- OIG Provider Self-Disclosure Protocol; CMS Self-Referral Disclosure Protocol.

Enforcement analytics examples as reported at the HCCA Data & Analytics Meeting (Mar. 2026). Citations provided for reference and educational use; not an exhaustive list.

Auditing & Monitoring: Takeaway Toolkit

Companion materials to "Scalable Technology-Enabled Auditing & Monitoring for Health Care Compliance"

WHAT IS IN HERE

1. Score Your Own Program — ten questions to answer honestly before someone else asks them.

2. Escalation — the triggers, the first five moves, and model policy language you can adapt.

3. Analytics Vendor Diligence — the contract terms that protect you when monitoring lives on someone else's platform.

4. Primary Sources — where every figure in the presentation came from, so you can check it yourself.

HOW TO USE THIS

Start with the score card. Answer the ten questions in your head, honestly.

Whatever you could not answer yes to is your workplan.

Pages 3 and 4 are starting points. Consider your own definitions and reporting lines.

Molly VandeVoort, Associate
Holland & Hart LLP | August 2026

Questions welcome: msvandevoort@hollandhart.com | T (208) 383-3964

1. Score Your Own Program

Ten questions. Answer them honestly — nobody is grading this.

01 Can you produce the plan and prove you executed it? _____

02 Does every activity have scope, criteria, and owner? _____

03 Can your records be queried across sites and years? _____

04 Does the plan trace to your current risk assessment? _____

05 Do findings have owners, deadlines, and closure? _____

06 Do you run outlier analysis on high-risk billing? _____

07 Do you know what OIG is working on in your lines? _____

08 Does your vendor contract cover data and exit? _____

09 Is routine monitoring separated from privilege? _____

10 Does your escalation path track the 60-day clock? _____

Fewer than eight yeses is not a failing grade. It is next year's workplan.

2. Escalation

Decide what the bad day looks like before it arrives.

ESCALATION TRIGGERS

- Signs of intentional misconduct or fraud
- Potential systemic overpayment, not isolated error
- Possible criminal, licensure, or media exposure
- Whistleblower or government inquiry on the same facts

THE FIRST FIVE MOVES

1. Pause the routine audit workflow
2. Engage counsel — privilege by design
3. Issue preservation notices; stop auto-deletion
4. Quantify exposure; scope the lookback
5. Make the reporting decision on the clock

THE 60-DAY CLOCK

"Identified" now uses the False Claims Act "knowingly" standard — actual knowledge, reckless disregard, or deliberate ignorance.

Deliberate ignorance means not looking can start the clock.

Up to 180 days to investigate related overpayments. Then 60 days to report and return.

§ 6 ESCALATION — MODEL POLICY LANGUAGE

If, during any audit or monitoring activity, facts suggest potential fraud, intentional misconduct, or systemic overpayment, the reviewer shall: (1) suspend the activity and cease further staff communications regarding the matter; (2) notify the Compliance Officer within one business day; (3) the Compliance Officer, in consultation with Legal Counsel, shall determine whether the matter proceeds as an investigation under attorney-client privilege; (4) preservation notices shall issue to all relevant custodians and automated deletion shall be suspended; and (5) any identified overpayment shall be quantified and resolved consistent with the 60-day repayment rule and applicable self-disclosure protocols.

Adapt before you adopt. Your definitions, reporting lines, and disclosure decisions have to be yours. | 42 U.S.C. § 1320a-7k(d); OIG Provider Self-Disclosure Protocol; CMS Self-Referral Disclosure Protocol.

3. Analytics Vendor Diligence

When monitoring lives on someone else's platform, the contract is a compliance control.

- ☐ Business Associate Agreement
  Compliant BAA executed before any PHI flows.
- ☐ Data ownership & portability
  You own the data and the outputs, in a usable format.
- ☐ Permitted use
  No secondary use; no model training on your PHI.
- ☐ Security & subcontractors
  Named standards, breach notice, flow-down terms.
- ☐ Model transparency & change control
  Notice of model changes; versioning you can reconstruct.
- ☐ Audit & cooperation rights
  Audit, government inquiry, IRO review, e-discovery.
- ☐ Explainability on demand
  Can they defend a flag to a regulator, in writing?
- ☐ Service levels & continuity
  Uptime, support, business continuity, disaster recovery.
- ☐ Exit & records return
  Your data back, in a usable format, on a defined clock.
- ☐ Regulatory change tracking
  Who watches the rules that govern the monitored activity?

You can outsource the platform. You cannot outsource the obligation — you still own the schema and the defensibility.

4. Primary Sources

Topic	Source	What it gives you
Program expectations	OIG General Compliance Program Guidance (Nov. 2023)	The seven elements and what an effective program looks like. Monitoring and auditing show up throughout.
Program expectations	DOJ, Evaluation of Corporate Compliance Programs (updated Sept. 2024)	The closest thing to a scoring rubric. Read the data analytics and AI governance sections.
Enforcement analytics	DOJ, National Health Care Fraud Takedown (June 23, 2026)	455 defendants, over $6.5B in false claims, and the Data Fusion Center.
Qui tam risk	DOJ Civil Division, Press Release 26-423 (Apr. 30, 2026, Updated July 17, 2026)	The FOCUS initiative — DOJ prioritizing outside data miners as relators.
Prior authorization	CMS, WISeR Provider and Supplier Operational Guide v7.0 (July 30, 2026)	Which services, which states, and how non-affirmations must be reviewed.
Your own risk areas	HHS-OIG Work Plan (oig.hhs.gov)	Download it as a dataset, not a webpage. Filter to active items in your programs.
If prevention fails	OIG Corporate Integrity Agreements (oig.hhs.gov)	2026 agreements now carry a generative AI disclosure clause. Read a recent one.

Molly VandeVoort, JD, MPH | Holland & Hart LLP | msvandevoort@hollandhart.com | T (208) 383-3964