

Navigating a New Era of Oversight

What Health Plans Need to Know

This white paper draws from insights shared during CERIS's recent Becker's Healthcare webinar, "Regulatory Pressures and Compliance Modernization: What Plans Need to Know." Panelists included Cereasa Horner, Director of Policy and Payment Integrity at CERIS, Steven Hamilton, Partner at Crowell & Moring LLP, and Payal Nanavati, Counsel at Crowell & Moring LLP. Together, they discussed how the Centers for Medicare & Medicaid Services (CMS) is intensifying its oversight of health plan payments—and what payers can do now to prepare.



Introduction: Increased Government Scrutiny

In recent years, government oversight of health plan payments has intensified significantly. Federal agencies are prioritizing the detection and correction of improper payments within Medicare Advantage (MA) and other risk-based programs, leading to an unprecedented level of CMS audit and enforcement activity.

At the center of this scrutiny is risk adjustment, the process by which MA plans are reimbursed based on the medical complexity of their members. Payments vary depending on the diagnosis codes submitted, most of which originate from providers. CMS aggregates these codes into Hierarchical Condition Categories (HCCs) that aim to reflect each member's health status and expected costs.

To verify the accuracy of those payments, CMS conducts Risk Adjustment Data Validation (RADV) audits, which are its primary enforcement tool for identifying and recovering overpayments. These audits examine whether diagnosis codes submitted by plans are adequately supported by medical records. While RADV audits have been ongoing for years, enforcement has increased considerably.

The challenge for payers is that CMS has not yet provided full clarity on how it will apply or interpret certain RADV methodologies going forward. Despite this uncertainty, the expectation is clear: audits are happening, and payers must be prepared.

“Even compared to just five years ago, government activity has ramped up significantly. A key example of that is the increased enforcement by the current administration and its prioritization of Medicare Advantage risk adjustment and RADV audits.”

Steven Hamilton, Partner at Crowell & Moring LLP

Health plans should begin implementing processes, oversight practices, and documentation standards today that will withstand scrutiny tomorrow.



Cereasa Horner

Director, Policy & Payment Integrity
CERIS



Steven Hamilton

Partner
Crowell & Moring LLP



Payal Nanavati

Counsel
Crowell & Moring LLP

Why it Matters: The Importance of a Proactive Strategy

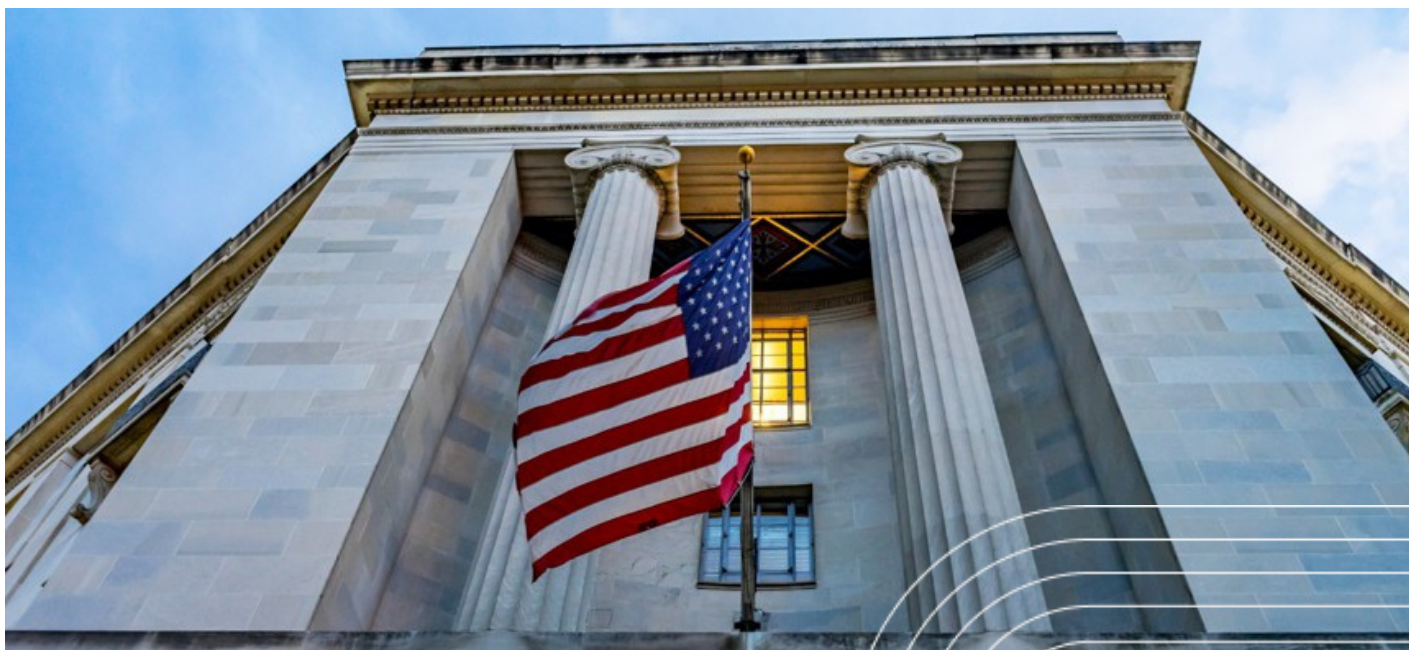
With heightened federal and state scrutiny of payments, health plans can no longer afford to take a reactive stance toward compliance. The audit activity seen today reflects a systemic shift toward continuous oversight and stricter enforcement. For payers, the implications are significant. A single audit finding can trigger financial recoupments, reputational damage, and even referral to enforcement agencies such as the Department of Justice (DOJ). Beyond the administrative burden, the consequences of noncompliance now carry greater potential for legal exposure under statutes like the False Claims Act.

“With federal and state healthcare programs, audits and inquiries from the government are not a matter of if, but when. It’s important to set a legal strategy at the outset of audit responses and activities.”

Payal Nanavati, Counsel at Crowell & Moring LLP

A proactive compliance strategy begins with recognizing that every audit request is a potential precursor to broader scrutiny. Unfavorable findings from CMS or the Office of Inspector General (OIG) may be referred to the DOJ for evaluation of a False Claims Act investigation—a step that can quickly escalate costs, penalties, and reputational harm.

By proactively integrating legal and operational strategy, payers can mitigate these risks before they materialize. Building the right compliance infrastructure early ensures that organizations are not just reacting to government inquiries but are actively shaping their preparedness for responses. The organizations that perform best under regulatory pressure are those that have embedded audit readiness into their daily operations and decision-making.



The Key Elements of an Effective Compliance Framework

Modernizing compliance infrastructure is now a critical priority for payers. A proactive compliance framework strengthens audit readiness and reinforces accountability across vendors, providers, and internal teams.

1. Set Legal Strategy Early in the Process

Legal teams should be involved from the outset of audit responses and government requests, not after findings emerge. They play a key role in identifying potential exposure, ensuring proper documentation, and pursuing available administrative remedies or exceptions. Early engagement allows organizations to build a strong record that can protect them if audit findings are later referred to enforcement agencies.

"The audit request you receive today can have major legal impacts for your company in the future. Your legal team can help you understand those legal and financial risks of adverse findings."

Payal Nanavati, Counsel at Crowell & Moring LLP

2. Strengthen Oversight and Policy Management

An effective compliance infrastructure requires consistent oversight of vendors and the creation of strong internal policies.

Audit Vendors

Payers must ensure the vendors that are responsible for coding or data submission operate under strict performance and compliance standards. Regular audits and performance monitoring are essential to maintain visibility.

Update Internal Guidelines

Internal coding and risk adjustment policies should be continuously updated based on the latest CMS guidance, ICD coding standards, and findings from internal and RADV audits. Policies should evolve as regulations shift and as your own data reveals trends or potential risks.

3. Prioritize Provider Education and Engagement

Another essential pillar of proactive compliance is provider education. Since most diagnosis codes originate with providers, payer compliance depends heavily on provider documentation accuracy. Providers should understand how their data submissions impact plan payments and audit exposure.

"[Coupling] your policy enforcement along with provider education allows a targeted focus to make sure that providers are submitting the correct information on the front end—rather than after a claim denial or audit request."

Cereasa Horner, Director of Policy and Payment Integrity at CERIS

Provider training should be complemented by a review of contract terms, ensuring that provider agreements include clear expectations around documentation, timeliness, and data accuracy.

4. Integrate Audit Readiness into Daily Operations

Audit preparation is an ongoing operational discipline, not a one-time task. Payers that embed compliance into daily workflows can identify issues early, prevent small errors from compounding, and demonstrate due diligence to regulators.

- **Conduct Ongoing Internal Audits:** Regularly review claims and documentation to detect inconsistencies or trends before they trigger external review.
- **Implement Coding Edits:** Address common errors such as modifier misuse or mismatched diagnosis and procedure codes through system-level coding edits and alerts.
- **Establish Feedback Loops:** Create structured communication channels between frontline staff, coding teams, compliance officers, and leadership. This ensures consistent policy enforcement and early awareness of emerging issues.

Avoiding Common Pitfalls: Strengthening Compliance Before Issues Arise

As CMS increases scrutiny of payment accuracy and diagnosis coding, common operational missteps continue to trigger audits and expose payers to regulatory and legal risk. Understanding where these issues occur and how to address them proactively can help organizations avoid costly enforcement actions.

Claims Documentation and Coding Missteps:

- **Downcoding and Unbundling:** Weak enforcement of policies often leads to inconsistent claims and billing errors.
- **Modifier Misuse and Code Mismatch:** Among the most frequent coding errors. Targeted internal audits can detect and correct these errors early.
- **Incomplete Claim Histories:** A comprehensive review of patient histories ensures accurate diagnosis reporting, especially for chronic conditions.
- **AI Inaccuracies:** Human oversight remains essential to interpret nuanced medical data and validate AI-assisted reviews.



CMS's Expectations: Diagnosis Coding and Chart Review

CMS's regulatory guidance has tightened expectations around diagnosis coding, chart reviews, and documentation integrity. Under recent rules, payers bear greater responsibility for ensuring that diagnosis codes submitted are fully supported by medical records. For RADV audits, this means payers should go beyond reviewing chronic conditions—they should also compare admitting versus final diagnoses and confirm whether each condition reported truly impacted the patient's care during the service period.

AI-assisted review tools can streamline this process but remain limited, as they cannot yet distinguish between a chronic condition from ten years ago and a current comorbidity affecting today's claim. Human review is still and will always be necessary to validate that coding accurately reflects the clinical reality.

Legal Implications of Overpayment Findings

Adverse findings can lead to False Claims Act exposure. Early legal engagement ensures procedural safeguards, preserves appeal rights, and documents compliance efforts. “Unintentional coding errors can turn into False Claims Act allegations if the conduct allegedly meets a threshold of knowledge—actual knowledge, reckless disregard, or deliberate ignorance,” Payal Nanavati noted. “What might start as isolated coding errors could collectively become an allegation of fraud if error rates are high or corrective action is lacking.” This underscores the importance of maintaining strong quality assurance processes to mitigate risk and demonstrate good-faith compliance.

The Ambiguity Challenge: Navigating Legal Uncertainty

CMS continues to refine audit methodologies and expand enforcement across risk adjustment and MA programs. Its discretion in extrapolating error findings adds another layer of uncertainty. Payers must demonstrate consistency and integrity in documentation, coding, and operational processes through well-defined protocols, internal monitoring, and vendor oversight.

As enforcement momentum builds, CMS’s focus on RA, RADV, and MA payment integrity will remain a top priority, with future policy shifts expected to sharpen fraud, waste, and abuse (FWA) oversight. To stay ahead, payers should maintain agile compliance programs, collaborate closely with legal counsel, and sustain ongoing provider education.



“As a payer, you really have to make sure that you have all of your processes and documentation in place to avoid those adverse determinations. You can always adapt and change policies, but you don’t want to be behind because of the RADV lookback period.”

Cereasa Horner, Director of Policy and Payment Integrity at CERIS

Overview: What Payers Can Do Today

With a clear understanding of common pitfalls and emerging regulatory expectations, the next step is turning compliance strategy into execution.

- ☐ **Evaluate Compliance and Risk Adjustment Programs Holistically:** Review your existing compliance framework and risk adjustment processes end-to-end. Identify areas for improvement.
- ☐ **Debrief and Learn from Prior Audits:** Analyze past CMS or OIG audit findings to refine policies, update provider education materials, and establish vendor performance expectations.
- ☐ **Reassess Provider and Vendor Relationships:** Establish clear accountability for coding accuracy, documentation, and claims submission. Define quality expectations, data-sharing requirements, and audit cooperation terms.
- ☐ **Prioritize Coding and Documentation Integrity:** Develop policies targeting high-risk areas, such as chronic condition coding, diagnosis validation, and the use of historical patient data.
- ☐ **Engage Legal and Compliance Teams Early:** Incorporate legal strategy into compliance planning from the outset to anticipate potential risks, pursue remedies, and build a defensible record.

Partnering for Proactive Compliance

Given the complexity and pace of CMS's evolving expectations, collaboration with experienced vendors has become a strategic necessity. Through a combination of policy intelligence, advanced data analytics, and clinical expertise, CERIS plays a pivotal role in helping payers close compliance gaps before claims are submitted.

CERIS supports payers in:

- Identifying potential risk areas through proactive data analysis and pattern recognition
- Providing policy and regulatory updates to ensure internal teams remain aligned with CMS guidance
- Delivering documentation and coding reviews backed by clinical professionals
- Enhancing vendor oversight and audit readiness

Conclusion: Sustaining Compliance Through Consistency

The compliance environment for health plans is becoming more stringent, data-driven, and transparent. CMS's heightened focus on payment accuracy represents a long-term shift toward continuous oversight.

For payers, success depends on integrating compliance into every layer of operations. By modernizing infrastructure, investing in provider and vendor collaboration, and leveraging partners like CERIS for insight and support, organizations can not only withstand CMS audits but also build stronger, more resilient payment systems for the future.

CERIS partners with payers across the nation to support their payment integrity programs and help them advance where they are in their journey.

Visit ceris.com to learn more.