WHITE PAPER

Top compliance priorities for U.S. healthcare payer organizations in 2026

Delivering strategic insights and practical guidance for health plan compliance leaders

By Leyla Erkan, Managing Director, Global Healthcare Legal, Risk & Compliance Practice Leader and Megan Allison, Associate Director, Global Healthcare Legal, Risk & Compliance Payer Practice Leader

protiviti®
Global Business Consulting

Table of contents

Introduction

As we enter 2026, the healthcare landscape is defined by regulatory ambiguity, growing operational complexity and financial pressures requiring organizations to be more compliance focused than ever. Navigating through sweeping legislation such as the One Big Beautiful Bill Act (OBBBA), Inflation Reduction Act of 2022 and state-level laws, coupled with legal challenges to federal rules such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule to Support Reproductive Health Care Privacy and the 2023 Medicare Advantage (MA) Risk Adjustment Data Validation (RADV) final rule are forcing organizations to pivot quickly and adapt strategically while exercising prudent caution to maintain stability and compliance. Chief compliance officers play a vital role in leading their organizations through complex environments with foresight and integrity. They face the unique challenge of inspiring stakeholders to uphold ethical and compliant practices, even amid an administration focused on deregulation and reducing the perceived burden of legal and regulatory requirements.

Amid this regulatory flux, the healthcare industry faces mounting pressure to remain profitable. The financial impact of major bills like OBBBA, projected to reduce federal healthcare spending by $900 billion over the next decade, has forced health plans (and providers) to reassess their business models, operational workflows and risk management strategies.[1] Chief compliance officers must balance the imperative to safeguard organizational integrity and regulatory alignment with the need to sustain financial performance in an environment of shrinking margins, increased audits and intensified program integrity measures. Successfully managing this with fewer staff and emerging technologies such as the explosion of artificial intelligence (AI) requires chief compliance officers to work smarter, leverage automation and prioritize high-impact risks through greater strategic oversight.

[1] *"Allocating CBO's Estimates of Federal Medicaid Spending Reductions Across the States: Enacted Reconciliation Package," Kaiser Family Foundation (KFF), July 23, 2025:* www.kff.org/medicaid/allocating-cbos-estimates-of-federal-medicaid-spending-reductions-across-the-states-enacted-reconciliation-package/.

Regulatory risk continues to place among the top ten concerns in our Executive Perspectives on Top Risks 2026 report, rising from sixth place last year to second place this year in the ranking of most significant short-term (two to three years) concerns and risks on the minds of healthcare industry leaders.

Regulatory excellence across plan operations is also a key priority for Internal Audit departments as shown in the recent Healthcare Internal Audit Plan Priorities Study, conducted by Protiviti and the Association of Healthcare Internal Auditors (AHIA). The results of that study show that the top five payer-specific priorities for Internal Audit departments are claims processing, member impact and access to care, provider relationships, product and sales, and risk adjustment/coding.[2]

Chief compliance officers stand at the forefront of integrity and accountability, championing robust internal controls, transparent reporting and a culture of ethical awareness across the enterprise. In an environment defined by constant change, proactive governance, collaboration and continuous monitoring are vital to remain aligned with evolving expectations and to protect both members and organizational trust. By leading with agility, courage and purpose, chief compliance officers empower their organizations to face uncertainty with confidence, uphold the highest standards of integrity and build a foundation for sustainable success.

This guide is designed to help health plans proactively identify and address their most critical compliance priorities. It focuses on strengthening oversight not only within the core responsibilities of a Compliance department but also across operational areas where regulatory risk often emerges. By providing practical strategies and insights, this resource supports chief compliance officers in building programs that are effective, adaptable and aligned with evolving regulatory expectations.

Protiviti
January 2026

[2] "2025 Healthcare Internal Audit Survey," Protiviti, 2025: www.protiviti.com/us-en/survey/2025-healthcare-internal-audit-survey.

Overview of payer compliance priorities
Compliance program effectiveness
Vendor and first-tier, downstream or related-entity oversight
Privacy and security
One Big Beautiful Bill Act
Fraud, waste and abuse
Impacts of artificial intelligence
Prior authorizations, appeals and grievances
Provider directories
Risk adjustment
Pharmacy benefit manager oversight
Encounter management

Please note that these priorities are not listed in order of importance.

As compliance challenges intensify, success hinges on smarter oversight, automation and a culture of integrity that withstands constant change.

Compliance program effectiveness

For health plans, "effective" is a standard that regulators expect and enforcement agencies measure. The U.S. Department of Health and Human Services (HHS) Office of Inspector General's (OIG) *General Compliance Program Guidance* (GCPG) set forth seven elements as the backbone of an effective program which serves as the benchmark by which programs are often evaluated.[3] The Centers for Medicare & Medicaid Services (CMS) likewise requires Medicare Advantage (MA) and Part D sponsors to implement the seven elements, extending obligations across First Tier, Downstream and Related Entities (FDRs), and expects plans to track and document program effectiveness.[4]

In 2026, CMS will pilot a new approach to assessing the effectiveness of Medicare Advantage and Part D compliance programs. Rather than relying solely on the current compliance program effectiveness protocol, CMS will engage Compliance departments in detailed discussions during program audits to evaluate how monitoring, prevention and corrective actions support adherence to CMS requirements. This shift emphasizes the importance of a robust, well-documented compliance program that can clearly demonstrate its impact on mitigating noncompliance.

[3] "General Compliance Program Guidance," U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG), November 2023: oig.hhs.gov/compliance/general-compliance-program-guidance/.

[4] "Medicare Managed Care Manual, Chapter 21 – Compliance Program Guidelines," Centers for Medicare & Medicaid Services (CMS), updated January 11, 2013: www.cms.gov/regulations-and-guidance/guidance/manuals/downloads/mc86c21.pdf.

While the terminology varies between regulatory bodies, the underlying requirements are the same, including written policies, procedures and standards of conduct; compliance leadership and oversight; effective training and education; effective lines of communication and non-retaliation; well-publicized disciplinary standards; risk assessment, auditing and monitoring; and prompt response, investigations and corrective actions.

Compliance strategies to demonstrate and improve effectiveness

- **Strengthen governance and tone at the top:** Ensure the chief compliance officer has direct, unfiltered access to the board of directors and compliance committee. The chief compliance officer must also maintain regular executive-level reporting on program performance and document oversight in minutes and dashboards to align with regulatory emphasis on leadership engagement and the Federal Sentencing Guidelines requirement for knowledgeable governing authorities exercising reasonable oversight.
- **Codify policies and test adoption:** Maintain a current code of conduct and policy suite that operationalizes regulatory duties (e.g., Chapter 21 of the Medicare Managed Care Manual) and incorporates annual risk assessment updates. Evaluate adoption of AI-enabled tools to monitor regulatory changes and regularly review policies for consistency and required updates. Store policies in an area where they can be easily accessed by the entire organization, and evidence policy awareness via attestations and periodic checks.

Compliance strategies at a glance

- Strengthen governance and tone at the top
- Codify policies and test adoption
- Deliver role-based training
- Enable speak up culture and protected reporting
- Audit and monitor using a risk-based plan
- Respond, remediate and verify closure
- Measure and evidence effectiveness

- **Deliver role-based training:** Ensure tailored training is conducted for roles in key areas such as claims, utilization management (UM), appeals and grievances, pharmacy, and risk adjustment. Ensure tailored training is conducted for roles in key areas such as claims, utilization management (UM), appeals and grievances, pharmacy, and risk adjustment. Track completion of training and require FDR training or attestations consistent with CMS guidance. Use refresher modules when rules change or audits reveal gaps, and consider applying AI to personalize content for each role.
- **Enable speak up culture and protected reporting:** Maintain confidential, anonymous reporting channels and emphasize non retaliation for good faith reporting to foster internal reporting of potential issues. Trend hotline metrics (e.g., volume, substantiation, cycle time) and key themes, potentially leveraging AI for analysis, to show effectiveness in practice.
- **Audit and monitor using a risk-based plan:** Build an annual work plan utilizing a risk assessment, and prioritize operational risks (e.g., benefit administration, grievances and appeals, claims payment accuracy, risk adjustment, network adequacy, formulary management). Leverage analytics and predictive compliance scoring using machine learning to detect anomalies and high-risk areas. Refresh the risk assessment and work plan as needed, but at least annually, to identify and address vulnerabilities proactively. Partner with Internal Audit and operational areas to embed the Institute of Internal Auditors' (IIA) Three Lines Model[5] to clarify first line ownership, second line compliance oversight, and third line independent auditing and assurance.
- **Respond, remediate and verify closure:** Standardize investigation protocols, root cause analyses, and corrective action plans to incorporate owners and timelines. Utilize standardized documentation and centralized storage of all activities, potentially through a technology solution such as a governance, risk management and compliance (GRC) system. Perform effectiveness checks, such as documentation review and retesting, after corrective actions are completed.

[5] "The IIA's Three Lines Model — An Update of the Three Lines of Defense," The Institute of Internal Auditors (IIA), July 2020: www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf.

- **Measure and evidence effectiveness.** Conduct periodic, independent effectiveness reviews that assess structure, operations and outcomes against the seven elements. Track leading/lagging indicators (e.g., training completion, hotline responsiveness, corrective action plan aging, audit issue recurrence, FDR findings, overpayment cycle times) and present trends to the board and compliance committee. Consider utilizing an AI-enabled compliance dashboard to track performance for real-time reporting.

In today's enforcement climate, effectiveness is the differentiator between a program that exists on paper and one that prevents issues, withstands audits and earns credit with regulators. Effective compliance programs empower staff to make compliant decisions, reduce regulatory risk and continuously strengthen program integrity across the organization. HHS-OIG's refreshed guidance, CMS's long standing Chapter 21 requirements, and the Federal Sentencing Guidelines converge on the same point: health plans that continuously test, evidence and improve their compliance programs are best positioned to protect members, maintain trust and avoid costly disruptions.

Vendor and first-tier, downstream and related-entity oversight

Effective oversight of vendors and delegated entities, including FDRs, is essential for health plans seeking operational efficiency and cost containment. Vendors perform critical functions such as claims processing, utilization management (UM), pharmacy benefits management, supplemental benefits, credentialing and member communications. However, as regulatory expectations intensify and the healthcare landscape evolves, the compliance risks associated with delegation are expanding.

Health plan responsibility extends beyond the delegation of operational tasks to vendors, as regulators continue to hold plans accountable for the actions and failures of their delegates. Recent high-profile data breaches and operational failures among third-party vendors have underscored the increased risk of reputational harm, regulatory penalties and member disruption.[6] The scope of delegation oversight now includes not only traditional compliance risks such as privacy and regulatory compliance, but also emerging concerns such as cybersecurity, AI governance and financial integrity. Compliance departments must proactively assess both established and evolving risks, including the ethical and operational implications of new technologies and offshore arrangements.

[6] "Change Healthcare Cybersecurity Incident Frequently Asked Questions," U.S. Department of Health and Human Services (HHS), March 14, 2025: www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html.

Oversight complexity is compounded by resource limitations and skill gaps within Compliance departments. Compliance and Delegation Oversight department staffing is often not scaled up as a health plan's delegated activities grow. Many departments lack the specialized expertise necessary to conduct delegate-specific reviews, especially in areas such as pharmacy benefit management, behavioral health and digital health platforms. Additionally, contracts with delegates often lack robust audit rights, data access provisions and clear performance metrics, limiting the health plan's ability to enforce accountability, especially for pharmacy benefit managers (PBMs).

As health plans increasingly delegate responsibilities, it is essential to exercise heightened caution when selecting vendors, particularly with supplemental benefit vendors and value-based care arrangements. The use of vendors that lack appropriate experience, resources or operational maturity can result in noncompliance with CMS and state-level requirements, leading to member disruption and inaccurate reporting. Compliance departments should implement rigorous due-diligence processes to assess vendor infrastructure, regulatory awareness and readiness before onboarding. Additionally, when considering offshore vendors, chief compliance officers must thoroughly review international, federal and state regulations to confirm their use is permissible and identify any additional oversight requirements.

Compliance strategies for vendor and FDR oversight

Compliance departments must have robust delegation oversight programs and be actively involved in pre-delegation reviews and contracting processes. Active participation helps identify potential compliance risks early and ensures appropriate safeguards are built into delegation agreements. Key compliance strategies include the following:

Compliance strategies at a glance

- Perform delegation oversight
- Participate in pre-delegation and contract reviews
- Enact regulatory change management
- Implement audit readiness protocols

- **Perform delegation oversight:** Establish and maintain a robust delegation oversight program. The delegation oversight program should include oversight of the delegate's compliance program, performance of regular delegate risk assessments using machine learning to analyze vendor data to predict compliance issues, and comprehensive delegate auditing and monitoring work plans. Use a centralized vendor management portal to track delegate compliance, contracts and attestations, and to provide a collaboration platform for instant vendor communication and issue escalation. Implement real-time vendor metrics dashboards with threshold alerts for noncompliance. Conduct delegate onboarding audits immediately upon go live to validate operational readiness and confirm regulatory alignment.
- **Participate in pre-delegation and contract reviews:** Coordinate with subject-matter experts from all impacted domains during vendor selection and onboarding to ensure that compliance risks are identified and addressed early, and that vendors meet all regulatory and operational expectations. Review delegate contracts prior to finalization to confirm the inclusion of audit rights, data transparency clauses and termination provisions.
- **Enact regulatory change management:** Develop structured processes to track delegate-related regulatory changes and interpret their impact, potentially employing AI to reduce manual effort. Communicate requirements to relevant stakeholders, provide targeted training and conduct periodic audits to verify the effective implementation of new rules. Conduct routine risk assessments focused on vendors and delegated activities to identify high-risk entities and monitor mitigation efforts.

- **Implement audit readiness protocols:** Implement mock audit processes that simulate actual audit scenarios to ensure delegates are prepared for regulatory audits, and refine processes for presenting information to regulators. For MA plans, it is essential that delegates regularly provide universes of data to the health plan, allowing Compliance departments to verify the accuracy and completeness of data extraction and reporting capabilities. Establish clear protocols for these audit readiness exercises, document findings, and require corrective actions where deficiencies are identified.

The use of delegates demands a sophisticated and proactive compliance strategy to ensure alignment with regulatory requirements and internal standards. Health plans must treat vendor oversight as a core compliance function, embedding compliance into every stage of the vendor lifecycle, from selection to performance monitoring. By doing so, health plans can protect members, meet regulatory obligations, strengthen program integrity, and maintain operational resilience.

Delegation may drive efficiency, but without rigorous oversight it opens the door to compliance failures, reputational harm and regulatory penalties.

Privacy and security

The security and privacy compliance landscape is experiencing a multifaceted transformation, driven by a rapidly evolving regulatory environment, intensifying cyber threats and rising consumer expectations. As the healthcare industry accelerates its adoption of digital technologies, privacy and security considerations have become central priorities for health plans nationwide. This dynamic environment, characterized by sophisticated cyberattacks, fragmented legal requirements and emerging technologies, demands proactive measures to identify, mitigate and manage risks effectively.

In response to the evolving healthcare landscape, the HHS Office for Civil Rights (OCR) has introduced sweeping revisions to the HIPAA Security Rule, with finalization and enforcement expected in 2026.[7] This update introduces a more prescriptive and rigorous framework for safeguarding electronic protected health information (ePHI). Key changes include mandatory annual compliance audits, enhanced Business Associate Agreements (BAAs), expanded risk assessments, encryption and multifactor authentication requirements for user access, incident response and contingency planning, and an overhaul of workforce training.

While HIPAA remains the federal baseline, state-level privacy laws are rapidly reshaping the compliance terrain for health plans. Currently, more than a dozen states have enacted comprehensive privacy laws that impose

[7] "HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information," U.S. Department of Health and Human Services (HHS), January 2025: www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html.

obligations beyond HIPAA. While certain state privacy laws provide specific carve-outs for covered entities governed by HIPAA, others may only offer exemptions specifically for protected health information (PHI) or may lack any carve-outs altogether. As a result, these laws place even more impetus on organizations to implement and maintain sound data governance practices.

Cybersecurity in healthcare has reached critical importance, as cyberattacks, including third-party breaches and credential theft have surged to unprecedented levels. Health plans are particularly vulnerable due to their reliance on complex vendor ecosystems and their central role in aggregating sensitive data. In this context, the 405(d) Health Industry Cybersecurity Practices (HICP) Framework has gained traction as a voluntary yet influential standard.[8] Aligning with HICP enables health plans to demonstrate proactive cybersecurity risk management, strengthen defenses across their networks, and maintain regulatory readiness in an increasingly hostile threat landscape.

Compliance strategies for privacy and security

By proactively aligning with regulatory updates, strengthening vendor oversight and embedding privacy and security into daily operations, Compliance departments can help safeguard sensitive health data while enabling innovation and trust. Privacy and security compliance professionals face unique challenges, and health plans must recalibrate their compliance strategies to remain resilient, trustworthy and legally sound. Key compliance strategies include the following:

- **Conduct regulatory and compliance assessments:** Perform comprehensive assessments to identify compliance gaps and inform strategic next steps to

[8] *"Health Industry Cybersecurity Practices (HICP)," U.S. Department of Health and Human Services (HHS) 405(d) Program, updated 2023:* 405d.hhs.gov/cornerstone/hicp.

Compliance strategies at a glance

- Conduct regulatory and compliance assessments
- Evaluate if and/or where AI models exist
- Evaluate minimum necessary/least privilege considerations
- Assess vendor risk management (VRM) for privacy and security
- Establish a robust reporting mechanism for enterprise compliance

prepare for potential regulatory changes. For example, now that the Notice of Proposed Rulemaking (NPRM) is issued for the HIPAA Security Rule, Compliance and Privacy departments should review the proposed modifications to better anticipate compliance gaps and operational changes in partnership with applicable business units such as mandatory asset inventories, network mapping, removal of flexible implementation specifications, enhanced risk analysis protocols and stricter incident response procedures. Using available guidance and tools (e.g., HIPAA Security Risk Assessment Tool), organizations can benchmark current policies, procedures and technical safeguards against proposed standards.[9]

- **Evaluate if and/or where AI models exist:** Collaborate with IT and/or Security departments to identify and understand if and where AI models are deployed. Consider leveraging AI detection technologies to enhance visibility, as understanding AI deployment is critical for assessing associated risks and meeting regulatory obligations. AI integration can significantly enhance cybersecurity by enabling predictive threat detection through advanced algorithms that analyze large datasets to uncover patterns and anomalies before breaches occur. Additionally, AI-powered systems can respond instantly to threats by isolating compromised devices or blocking malicious traffic, reducing damage and downtime. Continuously monitor user behavior for unusual activities, such as unauthorized access or data exfiltration to further strengthen defenses.
- **Evaluate minimum necessary/least privilege considerations:** Conduct regular comprehensive reviews of user access to environments that interact with ePHI. These reviews help ensure that individuals only have access to the specific data required to perform their job functions, thereby reducing the risk of unauthorized disclosure or misuse. Explore implementation of AI monitoring for user behavior and network traffic to spot breaches or improper PHI access in real time. Identify and remediate excessive or outdated privileges, enforce role-based access controls and align access policies with current regulatory expectations.

[9] "Guidance on Risk Analysis Requirements Under the HIPAA Security Rule," U.S. Department of Health and Human Services (HHS), updated July 2010: www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

- **Assess vendor risk management (VRM) for privacy and security:** Evaluate vendors' privacy and security policies and practices, as vendors can become entry points for cyberattacks. This includes validating the inclusion of strong data protection clauses in contracts and BAAs to enforce compliance with stringent standards. Collaborate with IT and/or Security departments to ensure a centralized system is in place to monitor vendor performance, track vulnerabilities and receive alerts on potential privacy and security risks to enhance oversight. Collaborate with vendors to establish clear protocols for incident response and breach management to ensure rapid containment and recovery.
- **Establish a robust reporting mechanism for enterprise compliance:** Implement integrated reporting systems that provide real-time visibility into privacy and security key performance indicators (KPIs). However, if integrating reporting systems is not a feasible approach, establish a clear and defined approach to stay abreast of your organization's privacy and security compliance across the enterprise through centralized dashboards to monitor progress, identify gaps and respond quickly to emerging risks. Establish cross-functional governance (i.e., bringing together IT, legal, operations and risk management) to ensure that privacy and security compliance is embedded across all business processes.

Health plans are navigating an intricate landscape shaped by increased federal scrutiny, state-specific regulations and growing consumer expectations for transparency and control over their data. Proactive strategies are necessary to strengthen the organization's privacy and security posture, support Compliance departments with privacy regulations, and reduce exposure to third-party threats. Chief compliance officers play a pivotal role in reevaluating traditional privacy practices and enacting innovative security strategies to address vulnerabilities and maintain compliance. Understanding and addressing key privacy and security concerns is critical for ensuring the security of ePHI while upholding trust and accountability.

One Big Beautiful Bill Act

OBBBA, enacted July 4, 2025, represents a fundamental shift in federal healthcare regulation and compliance risk. OBBBA is projected to reduce federal healthcare spending by $911 billion over the next decade, largely through stricter eligibility, new work requirements, and increased cost-sharing in Medicaid and Affordable Care Act (ACA) programs.[10] The Congressional Budget Office projects that these changes will result in 10 million additional uninsured Americans by 2034, with the most significant impact on Medicaid populations.[11]

For health plans, OBBBA introduces a complex array of new compliance requirements, especially for states that have expanded Medicaid coverage. Medicaid programs must now implement and monitor work requirements for many adults, conduct more frequent eligibility redeterminations and enforce shortened retroactive coverage periods. Adults who became eligible for Medicaid under the ACA expansion and who are above the poverty line will face new copays, and plans must ensure accurate application and tracking of these payments. The law also mandates new eligibility restrictions for noncitizens, prohibits Medicaid funding for certain provider types and services, and caps supplemental state-directed payments and provider taxes.

[10] "Allocating CBO's Estimates of Federal Medicaid Spending Reductions Across the States: Enacted Reconciliation Package," Kaiser Family Foundation (KFF), July 23, 2025: www.kff.org/medicaid/allocating-cbos-estimates-of-federal-medicaid-spending-reductions-across-the-states-enacted-reconciliation-package/.

[11] "Uninsured Data (Excel Dataset)," Congressional Budget Office (CBO), August 2025: www.cbo.gov/system/files/2025-08/61367-Uninsured-Data.xlsx.

In the ACA marketplace and private insurance sector, OBBBA standardizes enrollment periods, eliminates automatic reenrollment and imposes stricter verification for special enrollment periods and subsidy eligibility. The removal of repayment caps for excess premium tax credits and the expansion of health savings account (HSA) eligibility require plans to adapt their enrollment, subsidy and communication processes. Medicare changes under OBBBA, while less extensive, include a temporary increase in the physician fee schedule, reimposed Disproportionate Share Hospital (DSH) payment cuts, new eligibility restrictions for certain noncitizens, and adjustments to the Medicare drug price negotiation program. Across all federal healthcare programs, OBBBA heightens the focus on program integrity and fraud prevention, necessitating enhanced audits and data checks to prevent improper payments, especially for deceased or ineligible individuals.

While OBBBA's primary focus is on health plans, provider organizations will face significant downstream compliance and operational challenges. Providers will likely see increased uncompensated care and financial strain due to rising uninsured rates and reduced Medicaid enrollment. Safety-net and rural providers are particularly vulnerable to cuts in supplemental payments and provider taxes, while new compliance requirements affect providers of reproductive and gender-affirming care. At the same time, OBBBA creates opportunities for rural providers through new federal funding streams, but accessing these funds will require careful compliance with grant requirements and federal guidelines.

While many statutory provisions are proceeding as scheduled, several healthcare-related measures have experienced delays due to built-in statutory deferrals, administrative postponements or ongoing legal challenges. Additionally, some provisions are delegated to individual states for implementation, which may result in staggered enforcement and operational complexity across jurisdictions. The absence of timely federal agency guidance, particularly from CMS and HHS, has further delayed certain requirements, and the October 2025 federal government temporary shutdown introduced additional administrative disruptions. As a result, Compliance departments must remain vigilant, track evolving timelines and be prepared to adjust organizational readiness plans as new guidance and judicial decisions emerge.

Compliance strategies for OBBBA compliance

As OBBBA's sweeping reforms take effect, chief compliance officers play a critical role in guiding their organizations through a rapidly evolving regulatory landscape. Proactive planning and coordinated action are essential to ensure that all new requirements are understood, operationalized and monitored across business functions. Key compliance strategies include the following:

- **Conduct a comprehensive impact assessment:** Start by performing a thorough gap analysis comparing your organization's current operations to each new OBBBA requirement, identifying all affected business areas such as eligibility and enrollment, claims, provider networks, product design and billing. Involve cross-functional departments including legal, compliance, IT and operations to ensure all regulatory changes are fully understood and prioritized, and assign clear ownership for each compliance requirement. Document findings and action plans to provide evidence of due diligence.
- **Update policies, procedures, systems and training:** Confirm impacted areas translate each legislative change into updated internal policies, procedures and system configurations, ensuring that eligibility, disenrollment and cost-sharing rules are accurately reflected in operational workflows. Coverage policies and provider contracts should also be revised to incorporate new exclusions and payment structures and to implement claim edits to enforce retroactive coverage limits and service exclusions. Impacted areas should track all changes in a version-controlled manner and test system updates before deployment. Ensure delivery of comprehensive training for staff on new eligibility, disenrollment and claims processes, as well as creation of clear, timely communications for members and providers about coverage changes and compliance requirements. Use AI-driven scenario-based training modules, FAQs and multiple communication channels (such as email, intranet and webinars) to reach all stakeholders, and track training completion for compliance documentation.

Compliance strategies at a glance

- Conduct a comprehensive impact assessment
- Update policies, procedures, systems and training
- Collaborate with state and federal agencies
- Strengthen monitoring and auditing
- Update compliance program documentation
- Engage leadership and oversight bodies

- **Collaborate with state and federal agencies:** Engage proactively with Medicaid agencies and ACA exchanges to clarify implementation timelines, data-sharing requirements and any ambiguous provisions, all while establishing regular communication channels and participating in industry workgroups. Document all communications and regulatory guidance received and ensure your organization's processes are updated accordingly.
- **Strengthen monitoring and auditing:** Establish KPIs to track OBBBA-related disenrollments, subsidy denials and claims compliance, and conduct focused audits after KPI implementation to identify and address any issues. Leverage AI-enabled data analytics to detect trends or anomalies, perform mock regulatory reviews and document all corrective actions taken.
- **Update compliance program documentation:** Incorporate OBBBA into compliance risk assessments, annual work plans, and committee agendas, and revise policies to reflect new regulatory obligations and fraud prevention priorities. Update the compliance risk register to include OBBBA-specific risks and mitigation strategies and ensure that compliance committee minutes and board reports reflect ongoing oversight and progress.
- **Engage leadership and oversight bodies:** Regularly brief senior leadership, the compliance committee, and the board on OBBBA impacts, compliance strategies and progress, quantifying expected operational and financial impacts to support resource allocation. Use dashboards and executive summaries to communicate complex regulatory changes clearly, and provide updates on compliance milestones, challenges and resource needs.

OBBBA marks a new era of regulatory complexity and compliance risk for health plans and providers. Chief compliance officers must lead proactive, enterprisewide efforts to interpret the law, update practices and ensure adherence to new requirements. Early preparation, robust monitoring, and transparent leadership engagement are essential to navigating OBBBA's challenges, avoiding enforcement actions and safeguarding organizational integrity.

Fraud, waste and abuse

Fraud, waste and abuse (FWA) remains a foundational concern for health plan Compliance departments, and recent federal initiatives have elevated its importance to a critical priority. The U.S. Department of Justice (DOJ) and HHS have emphasized that healthcare fraud undermines public trust and depletes resources intended for patient care, and the CMS has indicated that it is committed to crushing fraud, waste and abuse.[12,13] In response, CMS has launched aggressive strategies such as expanded RADV audits, stronger use of technologies and analytics, enhanced interagency data sharing, and new models like the Wasteful and Inappropriate Service Reduction (WISeR) model to target wasteful and inappropriate services.[14] These developments underscore the need for chief compliance officers to stay abreast of evolving regulations, enforcement trends and leading practices. By understanding the key risk areas and implementing proactive controls, chief compliance officers can help safeguard organizational revenue, protect members and ensure alignment with federal expectations. Key FWA risks include the following:

- **Risk adjustment coding accuracy:** MA and ACA plans are reimbursed based on member risk scores, which are driven by documented diagnoses. Higher risk scores result in higher payments, creating an inherent

[12] "DOJ-HHS False Claims Act Working Group," U.S. Department of Justice (DOJ), Office of Public Affairs, July 2, 2025: www.justice.gov/opa/pr/doj-hhs-false-claims-act-working-group.

[13] "CMS Launches New Model to Target Wasteful, Inappropriate Services in Original Medicare," Centers for Medicare & Medicaid Services (CMS), Press Release, June 27, 2025: www.cms.gov/newsroom/press-releases/cms-launches-new-model-target-wasteful-inappropriate-services-original-medicare.

[14] Ibid.

incentive to capture additional or more severe diagnoses. While accurate coding is essential for proper reimbursement, practices such as upcoding or adding unsupported diagnoses can lead to inflated risk scores and significant overpayments — estimated at $17 billion annually.[15] These practices may constitute violations under the False Claims Act (FCA), exposing organizations to substantial legal and financial risk. As noted earlier, regulators have intensified scrutiny of risk adjustment practices, focusing on areas such as one-way chart reviews that add new diagnoses without removing unsupported ones, the use of health risk assessments (HRAs) to capture codes not substantiated elsewhere in the medical record, and failure to delete known erroneous codes. Plans are obligated to return improper payments once identified, and failure to do so within the 60-day overpayment rule can trigger FCA liability. Provider groups, particularly those in risk-sharing arrangements, also face exposure if unsupported coding trends emerge. Consequences range from whistleblower lawsuits and audits to civil penalties and even criminal charges.

- **Billing and coding schemes:** Traditional claims fraud schemes by providers or vendors remain a significant concern for health plans. Common tactics include upcoding services to bill for a more expensive service than was provided, unbundling procedures to charge separately rather than at a package rate, and submitting claims for services never rendered, often referred to as "ghost" or phantom claims. While the future of Medicare telehealth flexibilities is in flux, many health plans continue to offer telehealth benefits post the pandemic surge. The expansion of telehealth, while improving access, has also introduced new fraud and abuse vulnerabilities. Common schemes include "impossible day" billing, where providers report an implausible volume of telehealth encounters in a single day, and duplicate claims generated from one teleconsultation. And recent publications from the HHS-OIG highlight emerging risks tied to remote patient monitoring (RPM) and durable medical equipment linked to telehealth.[16,17] These patterns underscore the need for robust monitoring and enforcement

[15] "CMS Rolls Out Aggressive Strategy to Enhance and Accelerate Medicare Advantage Audits," Centers for Medicare & Medicaid Services (CMS), Press Release, May 21, 2025: www.cms.gov/newsroom/press-releases/cms-rolls-out-aggressive-strategy-enhance-and-accelerate-medicare-advantage-audits.

[16] "Consumer Alert: Remote Patient Monitoring," U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG), updated October 2023: oig.hhs.gov/fraud/consumer-alerts/consumer-alert-remote-monitoring/.

[17] "Justice Department Charges Dozens for $1.2 Billion in Health Care Fraud," U.S. Department of Justice (DOJ), Office of Public Affairs, Press Release, July 20, 2022: www.justice.gov/archives/opa/pr/justice-department-charges-dozens-12-billion-health-care-fraud.

strategies to safeguard program integrity. These abuses not only inflate healthcare costs but can harm members through unnecessary procedures or diverted resources. They also distort utilization data, potentially driving up premiums and exposing plans and providers to financial losses and audits aimed at recouping improper payments.

- **Prescription drugs:** Common pharmacy and drug-related schemes include opioid overprescription and diversion, doctor shopping, pharmacy billing fraud (such as charging for brand-name drugs while dispensing generics), and inappropriate formulary decisions influenced by kickbacks. The opioid crisis has elevated Part D opioid abuse to a national priority, as improper prescribing not only drives addiction but also results in significant financial costs. CMS requires Part D plans to maintain robust drug management programs to identify high-risk opioid utilizers and, when necessary, restrict them to designated prescribers or pharmacies. Enforcement agencies such as the HHS-OIG and Drug Enforcement Administration (DEA) aggressively investigate pill-mill operations and pharmacy fraud. Health plans must implement strong claims controls for pharmacy services, including quantity limits and prior authorization (PA) requirements for high-risk medications, while maintaining vigilant oversight of provider networks and PBMs. If network pharmacies or prescribers engage in fraudulent practices, plans can face CMS enforcement actions for failure to oversee FWA and may be required to repay substantial amounts. Beyond financial exposure, patient safety is at stake, as unchecked opioid dispensing can lead to harm for which plans may be held accountable under CMS patient protection standards.
- **Kickbacks and improper financial arrangements:** Kickbacks and other fraudulent inducements pose a serious threat to program integrity because they distort medical decision making and drive unnecessary costs. These schemes can involve providers receiving payments to refer patients or order specific drugs or tests, or vendors offering inducements to plan employees in exchange for favorable treatment.[18] While kickbacks are often associated with providers and pharmaceutical companies, health plans must also avoid entanglement in such arrangements, as claims resulting from

[18] "Health Care Plan Agrees to Pay Over $500,000 As Part of Self-Disclosure of Potential False Claims Act Violations," U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG), Enforcement Actions, 2025: oig.hhs.gov/fraud/enforcement/health-care-plan-agrees-to-pay-over-500000-as-part-of-self-disclosure-of-potential-false-claims-act-violations/.

kickback-tainted services are considered false claims under federal law. Regulators continue to enforce the Anti-Kickback Statute (AKS) and the Stark Law aggressively, with recent cases spanning traditional scenarios such as laboratory companies paying physicians for test referrals, to newer schemes, including health IT vendors bribing clients to induce utilization.[19] FDRs also face scrutiny; for example, PBMs must ensure that manufacturer rebate arrangements do not violate AKS. If kickback-related activity is discovered, health plans and providers may face retroactive claim denials, repayment obligations and potential civil or criminal penalties.

- **Waste and program inefficiencies:** Beyond outright fraud, wasteful practices in healthcare can significantly strain the system and increase costs. For example, CMS monitors spending anomalies such as the dramatic increase in Medicare spending on expensive "skin substitute" products used for wound care, which increased from $1.6 billion in 2022 to over $10 billion in 2024, raising concerns about potential overutilization and waste.[20] Further examples include unnecessary diagnostic tests, excessive office visits, and lack of care coordination that results in duplicative services. While often unintentional, these inefficiencies drive up premiums and increase costs for both CMS and health plans. CMS's Comprehensive Medicaid Integrity Plan emphasizes reducing improper payments, including those caused by waste and abuse.[21] Legislative efforts such as the OBBBA include provisions aimed at curbing waste by requiring stricter eligibility verification, removal of deceased or ineligible enrollees, and enhanced oversight of Medicaid and ACA programs.[22] CMS has also introduced rules to streamline PA and UM processes, with greater

[19] "Laboratory CEO, Marketers, and Physicians Pay Over $6 Million to Settle Allegations of Management Service Organization and Other Lab Testing Kickbacks," U.S. Department of Justice (DOJ), Office of Public Affairs, Press Release, September 8, 2025: www.justice.gov/opa/pr/laboratory-ceo-marketers-and-physicians-pay-over-6m-settle-allegations-management-service.

[20] "Medicare Program Integrity and Efforts to Root Out Improper Payments, Fraud, Waste and Abuse," Kaiser Family Foundation (KFF), October 2023: www.kff.org/medicare/medicare-program-integrity-and-efforts-to-root-out-improper-payments-fraud-waste-and-abuse/.

[21] "Comprehensive Medicaid Integrity Plan for Fiscal Years 2024–2028," Centers for Medicare & Medicaid Services (CMS), 2024: www.cms.gov/files/document/comprehensive-medicaid-integrity-plan-fys-2024-2028.pdf/.

[22] "H.R.1 — 119th Congress: Text of House Bill 1," Congress.gov, 2025: www.congress.gov/bill/119th-congress/house-bill/1/text.

transparency to ensure care remains medically appropriate.[23] Failure to manage waste can lead to operational inefficiencies, drains on clinical resources, increased administrative costs and regulatory audit findings; for example, a health plan that routinely pays for redundant tests may be flagged during a program audit for poor cost control. Health plans may need to upgrade enrollment systems to prevent coverage of ineligible individuals and refine claims review criteria to ensure payments are made only for necessary and efficient care.

- **Agent and broker marketing:** In April 2024, CMS published the 2024 Final Rule, introducing significant changes to MA agent and broker compensation structures intended to enhance transparency and protect beneficiaries from inappropriate marketing practices that could create conflicts of interest in plan enrollment.[24] These changes included redefining compensation to encompass administrative payments, prohibiting contractual or financial incentives that might compromise an agent's objectivity, and imposing stricter caps on payments. However, in July 2024, a federal court granted a temporary injunction pausing enforcement of most provisions, leaving the future of these rules uncertain.[25] Importantly, the injunction does not prevent CMS or other regulators from pursuing conduct they view as fraudulent or harmful to beneficiaries. Compensation structures that exceed fair market value, tie payments to a member's health status, or reward attainment of enrollment targets remain high risk and may violate the AKS. Such violations can lead to reputational damage, civil penalties and FCA penalties.
- **Prior authorizations:** While not traditionally categorized as a typical FWA topic, CMS and HHS-OIG have increasingly spotlighted inappropriate UM practices, particularly when plans deny medically necessary care to reduce costs, as a potential form of abuse. In 2022,

[23] "CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F)," Centers for Medicare & Medicaid Services (CMS), January 2024: www.cms.gov/cms-interoperability-and-prior-authorization-final-rule-cms-0057-f.

[24] "Medicare Program: Changes to the Medicare Advantage and the Medicare Prescription Drug Benefit Programs," Federal Register, Vol. 89, No. 79, April 23, 2024: www.federalregister.gov/documents/2024/04/23/2024-07105/medicare-program-changes-to-the-medicare-advantage-and-the-medicare-prescription-drug-benefit.

[25] "Court Strikes Down Key Medicare Marketing Regulations," Center for Medicare Advocacy, August 28, 2025: medicareadvocacy.org/court-strikes-down-key-medicare-marketing-regulations/.

an HHS-OIG report revealed that some MA plans denied services that should have been approved.[26] Further, the CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F) will require plans to streamline PA workflows and publicly report key metrics by 2026–2027.[27] These transparency requirements seek to improve patient access while also enabling regulators to identify outlier plans whose denial rates may signal problematic cost-saving measures at the expense of member care. Unjustified denials not only create compliance risk but can also lead to reputational harm, enforcement actions and potential civil penalties.

The evolving regulatory and enforcement landscape has concrete implications for health plan operations, internal controls and audit strategies. Proper oversight and education on FCA implications, combined with strong FWA reporting mechanisms and advanced data analytics, enables chief compliance officers to safeguard program integrity, reduce regulatory exposure and protect organizational reputation.

Compliance strategies to prevent and detect FWA

Effective FWA prevention and detection are core pillars of a strong Compliance department. These strategies promote ethical conduct, protect program integrity and ensure compliance with federal and state regulations. A proactive approach combines education, oversight and

Compliance strategies at a glance

- Strengthen special investigations units (SIUs)
- Conduct audits to identify potential FWA
- Evaluate provider network oversight
- Enhance internal reporting and issue response
- Oversee data and technology governance
- Ensure audit readiness

[26] "Some Medicare Advantage Organization Denials of Prior Authorization Requests Raise Concerns About Beneficiary Access to Medically Necessary Care," U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG), Report, April 27, 2022: oig.hhs.gov/reports/all/2022/some-medicare-advantage-organization-denials-of-prior-authorization-requests-raise-concerns-about-beneficiary-access-to-medically-necessary-care/.

[27] "CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F)," Centers for Medicare & Medicaid Services (CMS), January 2024: www.cms.gov/cms-interoperability-and-prior-authorization-final-rule-cms-0057-f.

accountability to reduce risk and maintain trust among members, providers and regulators. Key compliance strategies include the following:

- **Strengthen special investigations units (SIUs):** Equip SIUs with advanced data analytic tools to identify outlier billing patterns, integrate predictive modeling for early detection, and maintain strong collaboration with Claims, Provider Credentialing and Legal departments. Having a dedicated SIU is critical for health plans because it serves as the frontline defense against FWA, which can lead to significant financial losses, regulatory penalties and reputational harm. CMS explicitly requires MA and Part D plans to implement effective measures to detect and prevent FWA, and SIUs provide the specialized expertise and investigative capacity to meet this mandate.[28] Beyond compliance, SIUs help protect members from harm caused by fraudulent schemes, such as unnecessary procedures or unsafe prescriptions. Regular training, clear escalation protocols and periodic audits of SIU processes can further strengthen performance.
- **Conduct audits to identify potential FWA:** Adopt a proactive, multi-layered approach to mitigate FWA risks across health plan operations in partnership with the SIU. Implement AI machine-learning models and predictive analytics to recognize complex or emerging fraud patterns not caught by static rules. Conduct robust monitoring and auditing to evaluate medical record support of diagnosis codes and timely resolution of overpayments; identify anomalies like spikes in codes, excessive telehealth and redundant or duplicate claims; review prescribing patterns and drug management programs; and evaluate agent and broker compensation structures.
- **Evaluate provider network oversight:** Verify that credentialing processes include review of provider licensure and Medicare participation status and confirm that providers are not excluded or precluded from federal programs. Health plans must also have protocols to respond when a provider becomes the subject of fraud alerts or investigations, such as implementing enhanced claims review

[28] "Medicare Managed Care Manual, Chapter 21 — Compliance Program Guidelines," Centers for Medicare & Medicaid Services (CMS), updated January 11, 2013: www.cms.gov/regulations-and-guidance/guidance/manuals/downloads/mc86c21.pdf.

or restricting payment. Education is an often-overlooked preventive measure; providing network providers with training on proper billing and documentation standards, along with reminders about the plan's FWA reporting hotline, can reduce risk. Chief compliance officers should consider focused reviews of provider billing practices, such as annual audits of high-risk providers' claims against medical records to confirm coding accuracy. If claim payment or credentialing is delegated to an independent physician association (IPA) or vendor, delegation audits are critical to ensure those entities enforce FWA controls, as CMS holds plans accountable for failures by FDRs.

- **Enhance internal reporting and issue response:** Provide clear, accessible channels for employees and contractors to report suspected FWA, such as confidential hotlines and whistleblower protections, and maintain a defined investigation protocol that includes triaging issues, involving the SIU for FWA-related allegations and documenting every step of the process. When an issue is substantiated, prompt action is critical, whether referring criminal matters to law enforcement or self-disclosing and repaying overpayments. Plans are legally obligated to conduct reasonable inquiries without delay upon detecting potential FWA, and failure to act quickly can itself constitute a compliance lapse.[29] To prevent such issues, chief compliance officers should implement escalation timelines such as involving network management or considering suspension if a provider fails to comply within a set number of days.
- **Oversee data and technology governance:** Perform compliance oversight of emerging technologies such as advanced analytics and AI used in areas such as claims processing, fraud detection and UM to ensure these tools are used responsibly and in alignment with regulatory requirements. AI-driven FWA detection systems can significantly enhance monitoring capabilities, but they require rigorous validation to prevent bias and minimize false positives that could damage provider relationships or lead to inappropriate actions. Similarly, and as noted earlier, automation in UM must comply with CMS guidance, which mandates human clinician oversight and prohibits unexplainable denials. Chief compliance officers should collaborate closely with IT and Data Science departments to establish governance frameworks

[29] "Medicare Program Integrity and Efforts to Root Out Improper Payments, Fraud, Waste and Abuse," KFF, March 31, 2025. / www.kff.org/medicare/medicare-program-integrity-and-efforts-to-root-out-improper-payments-fraud-waste-and-abuse/

for AI, including transparency standards, periodic accuracy checks and clear documentation of decision logic. Additionally, with CMS interoperability rules expanding data sharing through application programming interfaces (APIs), chief compliance officers must ensure that FWA-related information such as provider terminations for cause or fraudulent National Provider Identifiers (NPIs) are communicated appropriately while maintaining privacy protections.

- **Ensure audit readiness:** Prepare for the FWA component of CMS program audits, which uses tracers to review how an FWA incident was handled end-to-end. Create clear case files that detail detection activities, investigation steps, resolution and corrective actions taken. Maintaining a comprehensive FWA log that tracks all issues and outcomes is essential. Consider implementation of an end-to-end FWA platform combining analytics, workflows, automated reporting and overpayment recovery tracking. Additionally, chief compliance officers should ensure that regular reporting to the compliance committee and the board includes FWA metrics such as the number of investigations, recoveries, disciplinary actions and self-disclosures. These reports not only demonstrate active management of FWA to regulators but also provide leadership with visibility into program integrity efforts.

The current, evolving regulatory landscape and heightened enforcement activity make robust FWA oversight an essential priority for health plan chief compliance officers. By implementing targeted controls across risk adjustment, billing, pharmacy, provider network management and agent compensation, health plans can proactively address areas of greatest FWA vulnerability. Leveraging technology, fostering cross-functional collaboration and maintaining rigorous documentation not only strengthen compliance but also demonstrate program effectiveness to regulators and enterprise leadership, while continuous education, regular audits and transparent reporting are key to sustaining a culture of integrity and accountability. Together, these actions ensure that the SIU and FWA practices function as a proactive safeguard that not only meets regulatory expectations but also reduces regulatory risk and preserves program integrity.

Impacts of artificial intelligence

AI is increasingly influencing health plan operations, from automating claim adjudication to enhancing risk adjustment accuracy. While most health plans are exploring or implementing AI systems and use cases, adoption varies across organizations.[30] As these technologies evolve, they bring both opportunities and complex operational and compliance challenges that require close monitoring. For Compliance departments, the question is no longer whether AI will impact their programs, but how to govern its use responsibly while mitigating regulatory, ethical and operational risks.

While AI innovations have the potential to improve efficiency, they also introduce the following distinct compliance challenges:

- **Claims adjudication:** AI-powered engines can expedite the claims adjudication process and reduce error rates by automating the review of claims. However, without robust oversight and governance, health plans risk noncompliance with federal and state regulations and guidelines. For example, automated decisions could overlook nuanced clinical scenarios, apply rules incorrectly, or be subject to hallucinations resulting in inappropriate denials or approvals. Compliance departments must continually validate that

[30] "NAIC Survey Reveals Majority of Health Insurers Embrace AI," National Association of Insurance Commissioners (NAIC), May 20, 2025: content.naic.org/article/naic-survey-reveals-majority-health-insurers-embrace-ai.

AI-driven processes align with regulatory requirements, maintain transparency in decision making, and provide mechanisms for appeals and manual review when necessary.

- **Fraud detection:** AI-driven analytics allow health plans to uncover anomalous billing patterns and provider behaviors in real time, reducing reliance on retrospective audits. This proactive approach strengthens payment integrity and accelerates recovery of improper payments. However, if these models are not properly designed, they may generate false positives (i.e., flagging legitimate claims as fraudulent), straining provider relationships and increasing administrative burden. Additionally, bias in profiling algorithms may disproportionately target certain provider types or geographic regions, raising fairness concerns. Effective governance requires ongoing monitoring, calibrated thresholds, transparent methodologies, and escalation protocols that balance fraud prevention with provider trust.
- **Risk adjustment:** AI-enabled tools allow health plans to review a large volume of medical records efficiently and can enhance the accuracy of risk scoring for MA and the ACA populations by quickly analyzing clinical and demographic information, as well as social determinants of health. With the complexity of these tools comes certain risks. For example, model drift can be caused by changes in coding practices or population health trends over time, which can degrade accuracy of the AI system or use case. Additionally, as AI tools lack true clinical understanding and may misinterpret context or nuances in medical records, health plans must ensure that any diagnosis code identified by AI is validated by a certified coder or clinician. Furthermore, the underlying data used to train the AI model or algorithms should be reviewed regularly for bias and drift.
- **Utilization management:** Health plans are increasingly turning to AI solutions to review coverage determinations to reduce administrative burden and speed decisioning, enabling faster access to care for members. CMS has issued guidance for MA plans that these technologies must account for individual patient history and needs, be overseen by a qualified human clinician and cannot deny coverage independently, be reviewed for bias, and must avoid discriminatory practices.[31] Additionally, opaque

[31] "Medicare Program Integrity: Oversight and Enforcement," Association of American Medical Colleges (AAMC), Report, 2023: www.aamc.org/media/74896/download?attachment.

algorithms that lack transparency, often called black-box models, may fail CMS audit standards because their decision making logic is not easily explainable to humans. This lack of explainability complicates compliance reviews and raises fairness concerns. To mitigate these risks, health plans must implement rigorous validation protocols, verify transparency and explainability of models and model outputs, and maintain auditable documentation for compliance reviews.

- **Member engagement:** Generative AI and conversational interfaces deliver personalized communication, guiding members through benefits, PAs and wellness programs. While these tools have the potential to improve satisfaction and adherence, they carry unique risks. Generative AI can produce inaccurate or fabricated responses, eroding member trust and creating compliance liabilities. Personalized interactions also require sensitive data, heightening exposure to privacy breaches and regulatory scrutiny under HIPAA and Federal Trade Commission (FTC) guidelines. Health plans must require strict data governance, validation of AI-generated content and human oversight for complex inquiries to ensure accuracy and protect member confidence.

Just as the implementation of AI is growing rapidly, so is the regulatory landscape. Recent state-level legislation, such as Texas House Bill 149, now mandates disclosure when AI is used in diagnosis or treatment.[32] While this law directly impacts providers, it signals a broader trend toward transparency and accountability in AI use across the healthcare ecosystem. In the health plan space, several states, including California, Maryland, Nebraska and Arizona, have enacted or proposed laws prohibiting AI as the sole basis for adverse determinations in PAs, requiring human review to safeguard patient rights.

At the federal level, several key regulations are shaping how health plans can employ AI technologies. The CMS Interoperability and Prior Authorization Rule introduces new standards for API-based PA workflows and mandates greater transparency in decision making, with phased implementation through 2027.[33] Additionally, section 1557 of the ACA, updated in 2024, now includes provisions about algorithmic nondiscrimination, requiring entities to assess and mitigate bias in AI tools.[34]

[32] "Texas House Bill 149 (2025 Session)," LegiScan, 2025: legiscan.com/TX/bill/HB149/2025.

[33] "CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F)," Centers for Medicare & Medicaid Services (CMS), January 2024: www.cms.gov/cms-interoperability-and-prior-authorization-final-rule-cms-0057-f.

[34] "HHS Issues New Rule to Strengthen Nondiscrimination Protections and Advance Civil Rights in Health Care," U.S. Department of Health and Human Services (HHS), April 26, 2024: www.hhs.gov/sites/default/files/aca-section-1557-press-release.pdf.

Further, the FTC's Health Breach Notification Rule (HBNR) expands breach reporting requirements to health technologies not covered by HIPAA, including many AI-powered apps and platforms.[35] If these tools collect personal health records (PHRs) and experience a breach, this may trigger notification obligations not only to individuals, but also the FTC and, in some cases, the media. HHS-OCR has also issued guidance on the use of tracking technologies, such as cookies and pixels, on healthcare websites and apps.[36] These tools, often embedded in AI-driven platforms, may collect PHI unbeknownst to the end user. HHS-OCR requires entities to either establish BAAs with tracking vendors or obtain explicit patient authorization before sharing PHI. Lastly, outside of federal requirements, many states have implemented laws that impact how health data may be used by AI-driven tools and technologies. For instance, Washington's My Health My Data Act (MHMDA) imposes strict consent requirements and even introduces a private right of action for violations, extending privacy protections to consumer health data outside traditional HIPAA frameworks.[37]

The National Institute of Standards and Technology (NIST) AI Risk Management Framework defines the six characteristics of trustworthy AI, which include the following:[38]

1. AI validity and reliability is promoted through ongoing monitoring that confirms an AI use case is performing as intended. Furthermore, AI risk management efforts should include manual reviews to mitigate errors in AI responses.

2. AI safety is improved through robust AI development processes, responsible use and decision making, and communication of risks based on historical experience. Existing cybersecurity mechanisms should be leveraged and enhanced to maintain confidentiality, integrity and availability of AI use cases to protect against adversarial attacks, data poisoning and exfiltration of information.

[35] "Health Breach Notification Rule," Federal Trade Commission (FTC), updated 2024: www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule.

[36] "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," U.S. Department of Health and Human Services (HHS), updated March 2024: www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[37] "Revised Code of Washington (RCW) 19.373 — Washington Foundational Data Privacy Act," Washington State Legislature, 2025: app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true.

[38] "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," National Institute of Standards and Technology (NIST), January 2023: www.nist.gov/itl/ai-risk-management-framework.

3. Transparency can be achieved by effectively defining and documenting the AI's design choices, training data characteristics, AI methodology and structure, and human interaction. Accountability requires clear lines of responsibility between humans and AI, where effective monitoring and governance can minimize potential harm or unintended consequences.
4. Health plans must ensure that AI systems are understandable, with clear explanations of data sources, algorithms and decision making processes to foster trust.
5. Protecting user privacy and handling sensitive data in accordance with legal and ethical standards is critical, as is implementing robust security measures to safeguard system integrity.
6. Proactively identifying and mitigating biases in data collection, model training and algorithmic decisions is essential to prevent unfair outcomes or discrimination.

Compliance strategies for AI governance and oversight

AI governance and oversight are essential to ensure that AI operates responsibly, ethically, and in accordance with regulatory requirements and leading practices. A robust governance framework establishes clear accountability for AI decision making, promotes transparency and safeguards against risks such as bias, privacy breaches and noncompliance. By integrating compliance controls throughout the AI lifecycle, from data collection and model development to deployment and monitoring, organizations can strengthen trust, uphold ethical standards and demonstrate regulatory readiness in an evolving legal and technological landscape. Key compliance strategies include the following:

Compliance strategies at a glance

- Develop policies and standards
- Implement AI governance
- Establish risk-based AI governance
- Require transparency and human-in-the-loop oversight
- Conduct audits
- Perform vendor due diligence
- Monitor regulations
- Create incident response plans

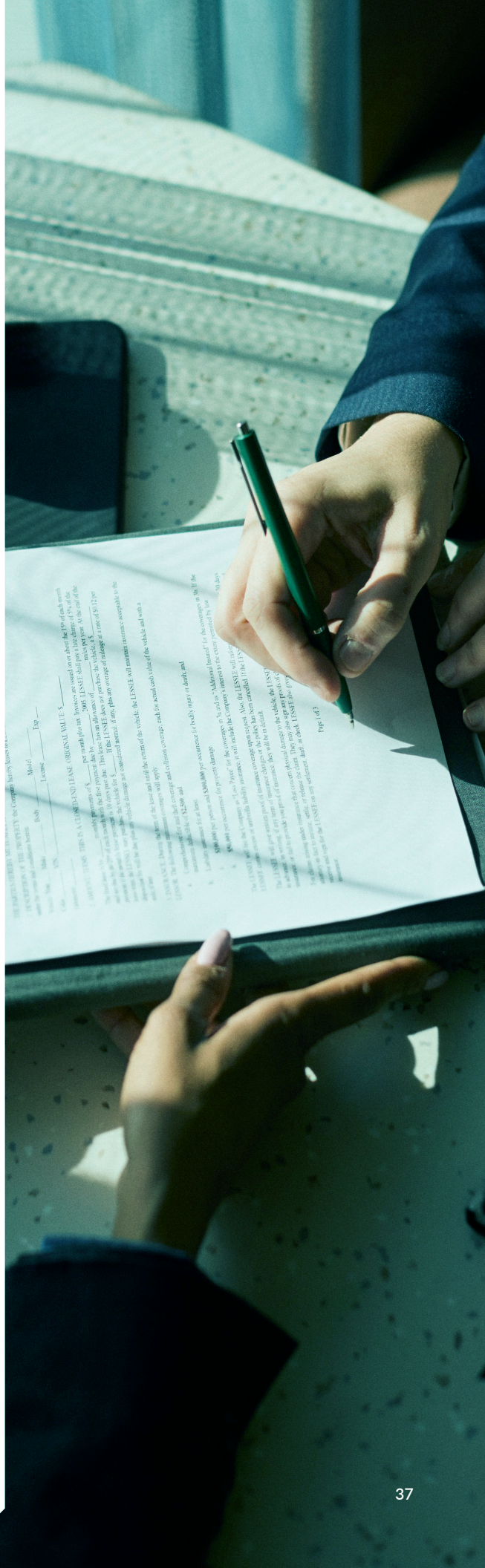
- **Develop policies and standards:** Oversee development of policies, rules and guidelines for AI governance, development, procurement, deployment and use. This foundational governance ensures alignment with ethical principles, regulatory expectations and organizational goals.
- **Implement AI governance:** Ensure there is a robust governance operating model with clearly defined roles and responsibilities, including a steering committee and/or board. This structure should integrate seamlessly with existing governance functions such as data privacy, cybersecurity and data governance to ensure alignment, eliminate redundancies and promote cross-functional collaboration. Key risk indicators (KRIs) and escalation protocols for algorithmic failures or compliance breaches should be used to minimize operational and reputational damage.
- **Establish risk-based AI governance:** Design and implement an AI intake process, along with a comprehensive inventory of models, use cases and systems. Additionally, apply a risk-tiering framework and risk assessment process to enable secure, compliant and strategically aligned adoption of AI. The level of oversight and control of each AI use case can be determined through this risk-based approach.
- **Require transparency and human-in-the-loop oversight:** Review AI tools to ensure they are explainable and documentation of model logic, inputs and limitations is maintained. For high-impact decisions, require manual oversight to prevent overreliance on automation and ensure appropriate clinical and regulatory judgment is applied.
- **Conduct audits:** Conduct regulatory compliance audits and align internal policies and procedures with requirements. Perform periodic fairness assessments across demographic groups and adjust models accordingly to prevent bias. Regularly evaluate AI systems, use cases and models for accuracy, reliability and compliance beyond bias detection. Measure and evaluate business performance over time and the effectiveness of controls.

- **Perform vendor due diligence:** Require all vendors to report any existing or planned use of AI in their processes. Demand transparency reports, bias audits and contractual safeguards for third-party solutions. Consider including reviews of vendor AI use as part of delegation oversight processes.
- **Monitor regulations:** Implement automated compliance tracking for state and federal mandates and legal updates around acceptable AI use. Ensure there is a framework for AI risk classification and assessment, KRIs, risk ownership, oversight and reporting.
- **Create incident response plans:** Define escalation protocols for system, model or algorithmic failures or compliance breaches to minimize operational and reputational damage.

As AI continues to reshape health plan operations, chief compliance officers are uniquely positioned to help guide its responsible adoption. The integration of AI into functions such as claims adjudication, UM, fraud detection and risk adjustment offers significant operational benefits but also introduces nuanced regulatory, ethical and operational risks. With the regulatory landscape rapidly evolving at both state and federal levels, passive oversight is no longer sufficient. Chief compliance officers must champion robust AI governance frameworks that prioritize transparency, fairness and accountability, while embedding AI risk into broader enterprise risk-management strategies. By proactively implementing controls, ensuring human oversight and fostering a culture of responsible innovation, chief compliance officers can help their organizations harness the power of AI while safeguarding regulatory integrity and member trust.

Prior authorizations, appeals and grievances

Timely and equitable access to medically necessary care is both a regulatory mandate and a core priority for health plans. Recent CMS changes for MA plans have heightened expectations for member access, requiring plans to align UM decisions with traditional Medicare coverage criteria. PA processes must now focus solely on confirming diagnoses and medical necessity, with new protections such as a 90-day transition period for members in active treatment and annual UM committee reviews to ensure policy consistency with Medicare rules.[39] Beginning January 2026, standard PA decisions must be made within seven calendar days, and approvals must remain valid for as long as medically reasonable and necessary to minimize care disruptions.[40, 41] In parallel, the CMS Interoperability and Prior Authorization Final Rule introduces requirements for faster decision making and greater transparency, including the implementation of APIs and public reporting of PA metrics.[42]



[39] "CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F)," Centers for Medicare & Medicaid Services (CMS), January 2024: www.cms.gov/cms-interoperability-and-prior-authorization-final-rule-cms-0057-f.

[40] Ibid.

[41] "Medicare Program: Changes to the Medicare Advantage and the Medicare Prescription Drug Benefit Programs for 2024," Centers for Medicare & Medicaid Services (CMS), April 5, 2023: www.cms.gov/newsroom/fact-sheets/2024-medicare-advantage-and-part-d-final-rule-cms-4201-f.

[42] "CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F)," Centers for Medicare & Medicaid Services (CMS), January 2024: www.cms.gov/cms-interoperability-and-prior-authorization-final-rule-cms-0057-f.

Member access is also shaped by appeals and grievances processes. CMS has extended the enrollee appeal filing period from 60 days to 65 days, updated model notices to reinforce fast-track rights, clarified integrated processes for Dual Eligible Special Needs Plans (D-SNPs), and emphasized the importance of granting appropriate appeal rights.[43, 44] Recent HHS-OIG reports have highlighted high rates of PA denials in Medicaid Managed Care and raised concerns about access to medically necessary care for MA members, signaling increased regulatory scrutiny of how plans manage PAs, appeals and grievances.[45, 46]

The use of algorithms and AI in UM is evolving rapidly. CMS has clarified that while AI may assist with coverage decisions, it cannot be the sole basis for denying, terminating or downgrading care. Plans must consider each member's unique clinical circumstances and adhere strictly to Medicare coverage rules.[47] CMS and HHS-OCR have also warned of the risks of discrimination and bias in AI-driven decision support tools, with Section 1557 of the ACA prohibiting discriminatory impacts and requiring plans to identify and mitigate such risks.[48] Together, these expectations mean health plans must pair innovation with strong governance to protect member access and equity.

[43] "Contract Year 2026 Policy and Technical Changes to the Medicare Advantage Program, Medicare Prescription Drug Benefit Program, Medicare Cost Plan Program, and Programs of All-Inclusive Care for the Elderly (CMS-4208-F)." Centers for Medicare & Medicaid Services (CMS), April 4, 2025: www.cms.gov/newsroom/fact-sheets/contract-year-2026-policy-and-technical-changes-medicare-advantage-program-medicare-prescription-final.

[44] "Medicare Managed Care Appeals & Grievances," Centers for Medicare & Medicaid Services (CMS), November 20, 2024: www.cms.gov/medicare/appeals-grievances/managed-care.

[45] "High Rates of Prior Authorization Denials by Some Plans and Limited State Oversight Raise Concerns About Access to Care in Medicaid Managed Care," Office of Inspector General (OIG), U.S. Department of Health and Human Services, July 17, 2023: oig.hhs.gov/reports/all/2023/high-rates-of-prior-authorization-denials-by-some-plans-and-limited-state-oversight-raise-concerns-about-access-to-care-in-medicaid-managed-care/.

[46] "Some Medicare Advantage Organization Denials of Prior Authorization Requests Raise Concerns About Beneficiary Access to Medically Necessary Care," Office of Inspector General (OIG), U.S. Department of Health and Human Services, April 27, 2022: oig.hhs.gov/reports/all/2022/some-medicare-advantage-organization-denials-of-prior-authorization-requests-raise-concerns-about-beneficiary-access-to-medically-necessary-care/.

[47] "Medicare Program Integrity: Oversight and Enforcement," Association of American Medical Colleges (AAMC), Report, 2023: www.aamc.org/media/74896/download?attachment.

[48] "HHS Issues New Rule to Strengthen Nondiscrimination Protections and Advance Civil Rights in Health Care," U.S. Department of Health and Human Services (HHS), Press Release, April 26, 2024: www.hhs.gov/sites/default/files/aca-section-1557-press-release.pdf.

Compliance strategies to ensure access and regulatory alignment

- **Track implementation of new guidance:** Establish robust tracking and oversight mechanisms, harnessing AI technologies, to ensure new regulations related to PAs and appeals are fully operationalized across all impacted business areas. This process should include reviewing and updating policies, procedures, training and communications for both internal staff and FDRs to ensure they are aligned with current regulatory expectations.
- **Perform audits to confirm compliance:** Conduct targeted audits covering new CMS guidance, including the CMS Interoperability and Prior Authorization Final Rule, the Contract Year 2026 MA and Part D final rule (CMS-4208-F), and recent appeals requirements. These audits should evaluate organizational readiness for upcoming implementations, identify performance gaps against revised criteria and drive timely corrective actions to ensure regulatory alignment and operational integrity.
- **Govern AI use in coverage decisions:** Strengthen governance procedures for AI in coverage decisions by validating bias testing, ensuring algorithm explainability and implementing Section 1557 nondiscrimination testing and vendor attestations. To safeguard clinical judgment and regulatory compliance, require human-in-the-loop oversight for all coverage determinations supported by AI.
- **Measure and evidence effectiveness:** Track and trend key access-related metrics such as PA and appeal processing timeliness, approval and denial reasons, overturn rates at each appeal level, grievance categories, continuity-of-care exceptions and API uptime/usage. Assess use of advanced tools such as AI-driven analytics to enhance metric tracking and accelerate identification of trends or systemic issues. Report these findings to the UM committee, compliance committee, and board, and use findings to drive corrective actions and targeted training.

Plans must pair strong UM governance with interoperability, timely decisions, transparent criteria, and equitable AI use. These actions ensure members receive timely access to medically appropriate care while enhancing the plan's ability to meet regulatory expectations, reduce avoidable delays, lower appeal and grievance volumes, and strengthen member trust and outcomes.

Compliance strategies at a glance

- Track implementation of new guidance
- Perform audits to confirm compliance
- Govern AI use in coverage decisions
- Measure and evidence effectiveness

Provider directories

Accurate provider directories are a cornerstone of regulatory compliance, member access and financial stewardship for health plans. Directories function as the primary reference for members seeking care, regulators evaluating network adequacy, and providers confirming participation status. When directories are inaccurate or outdated, the consequences can be significant, ranging from member harm and regulatory penalties to reputational damage and financial liability.

Regulatory scrutiny of provider directory accuracy has intensified at both the federal and state levels. The CMS and state agencies now require health plans to maintain directories that are not only current but also comprehensive. Notably, CMS audits of MA online provider directories revealed an average inaccuracy rate of nearly 45% by location.[49] Similarly, HHS-OIG reviews of MA and Medicaid Managed Care behavioral health directories found that many networks included a substantial proportion of inactive providers, resulting in "ghost networks" that appear to meet adequacy standards but fail to deliver sufficient access for members.[50] Recent enforcement actions, including fines, civil monetary penalties, enrollment suspensions and contract terminations, underscore the risks associated with noncompliance.[51]

[49] "Online Provider Directory Review Report," Centers for Medicare & Medicaid Services (CMS), November 28, 2018: www.cms.gov/medicare/health-plans/managedcaremarketing/downloads/provider_directory_review_industry_report_round_3_11-28-2018.pdf.

[50] "Many Medicare Advantage and Medicaid Managed Care Plans Have Limited Behavioral Health Provider Networks and Inactive Providers," Office of Inspector General (OIG), U.S. Department of Health and Human Services, October 2025: oig.hhs.gov/documents/evaluation/11233/OEI-02-23-00540.pdf.

[51] "Attorney General Bonta Secures $40 Million Settlement with Health Net for Misleading Consumers With Inaccurate Provider Directories," California Office of the Attorney General, Press Release, October 13, 2025: oag.ca.gov/news/press-releases/attorney-general-bonta-secures-40-million-settlement-health-net-misleading.

The No Surprises Act (NSA) imposes strict requirements on provider and health plan directories, with health plans facing daily penalties of up to $100 per affected individual for inaccurate listings and providers subject to fines of $10,000 per violation for failing to update information within two business days.[52] CMS's latest guidance for Medicaid and Children's Health Insurance Program (CHIP) plans mandates quarterly directory updates, expanded data elements and public access to online directories via API.[53] MA plans must now comply with new requirements under the 2026–2027 Final Rule 4208-F2, including updating provider data within 30 days, annual attestations of accuracy, and submission of data for CMS publication.[54] States have also adopted rigorous standards, for example, with California requiring weekly updates for online directories and other states mandating update frequencies ranging from 15 to 90 days.[55]

Given this landscape, chief compliance officers must lead proactive governance to ensure directory accuracy and mitigate enforcement risk. By investing in robust policies, technology and continuous improvement, chief compliance officers can transform provider directory management into a strategic asset that not only meets regulatory expectations but also safeguards member access and program integrity.

[52] "Coronavirus Aid, Relief, and Economic Security (CARES) Act, Public Law No. 116-260," U.S. Congress, July 4, 2025: www.govinfo.gov/content/pkg/COMPS-15754/pdf/COMPS-15754.pdf.

[53] "State Health Official Letter #24-003: Consolidated Appropriations Act, 2023 Amendments to Provider Directory Requirements," Centers for Medicare & Medicaid Services (CMS), July 16, 2024: www.medicaid.gov/federal-policy-guidance/downloads/sho24003.pdf.

[54] "Federal Register: Medicare and Medicaid Programs; Contract Year 2026 Policy and Technical Changes to the Medicare Advantage Program, Medicare Prescription Drug Benefit Program, Medicare Cost Plan Program, and Programs of All-Inclusive Care for the Elderly (PACE)-Finalization of Format Provider Directories for Medicare Plan Finder (CMS-4208-F2)," Centers for Medicare & Medicaid Services (CMS), September 19, 2025: www.federalregister.gov/documents/2025/09/19/2025-18236/medicare-and-medicaid-programs-contract-year-2026-policy-and-technical-changes-to-the-medicare.

[55] "SB 137 Provider Directory Standards," California Department of Insurance, Guidance Document, December 30, 2016: www.insurance.ca.gov/0250-insurers/0500-legal-info/0200-regulations/HealthGuidance/upload/SB137ProviderDirectoryStandards.pdf.

Compliance strategies for provider directory integrity

- **Establish rigorous policies and oversight:** Ensure implementation of clear, enforceable policies requiring timely updates and verification of provider data. Confirm that all required data elements are captured, including accessibility, languages and telehealth availability.
- **Utilize technology for data governance:** Consider use of advanced data management tools and APIs to automate updates and synchronize provider information across systems. Validate data sources and ensure interoperability with state and federal directories. Evaluate the use of AI tools to research current provider data and to identify potentially outdated listings.
- **Conduct ongoing auditing and monitoring:** Perform regular audits to verify directory accuracy, identify discrepancies and remediate errors. Explore potential advanced technologies such as AI-enabled analytics to detect patterns of inaccuracy, including providers listed as accepting new patients who are not currently accepting new patients and providers who are inactive.
- **Institute education and training:** Provide ongoing education for staff responsible for directory management, emphasizing regulatory requirements and the impact of inaccuracies on member access and compliance risk.

Today's regulatory environment underlines that precision in provider directory management is not optional; it is a strategic and regulatory imperative. The convergence of heightened governmental oversight, evolving technology and substantial financial penalties demands vigilant compliance leadership. By implementing robust governance, leveraging technology, and fostering a culture of accuracy and accountability, chief compliance officers can protect their organizations from exposure and reputational harm while ensuring members have reliable access to care.

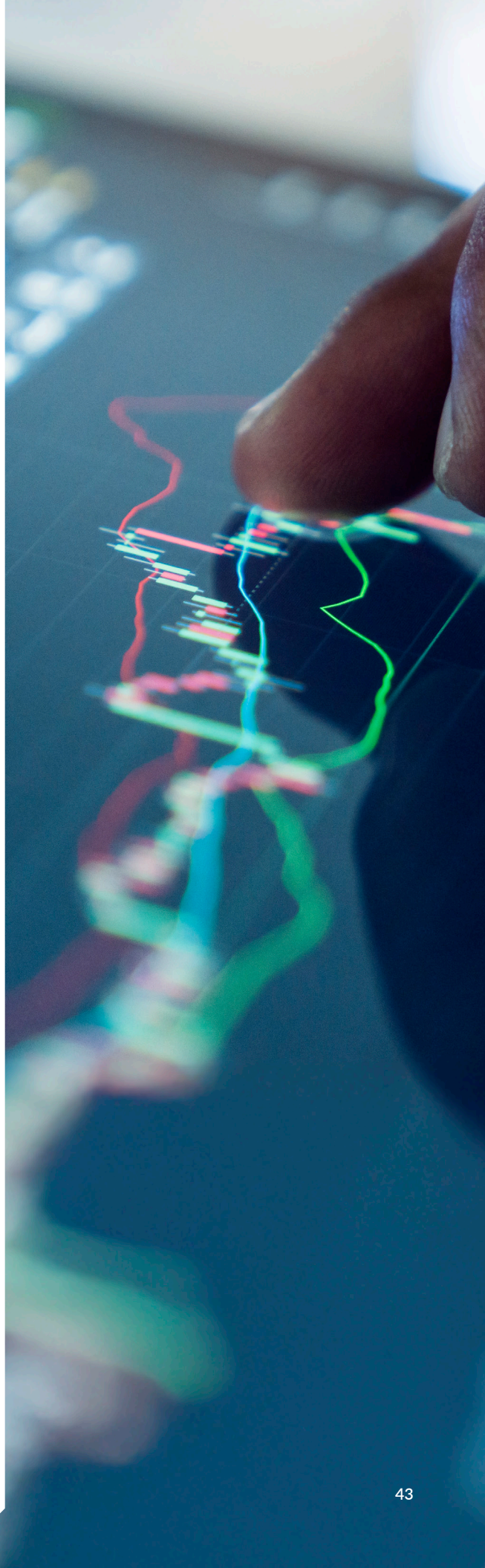
Compliance strategies at a glance

- Establish rigorous policies and oversight
- Utilize technology for data governance
- Conduct ongoing auditing and monitoring
- Institute education and training

Risk adjustment

Accurate risk adjustment coding is foundational to regulatory compliance and financial integrity for health plans and providers. Risk scores under MA and ACA plans directly influence payment levels and are intended to ensure that health plans and providers who care for sicker, higher-cost populations receive adequate reimbursement, while those caring for healthier populations are reimbursed accordingly. This prevents a financial incentive to avoid patients with complex health needs and promotes comprehensive care for all, helping to advance health equity. However, this payment model also introduces significant compliance risk, including the potential for inflated risk scores through unsupported diagnoses. When diagnoses submitted to CMS are not substantiated by medical documentation, the resulting overpayments can trigger reputational harm, civil money penalties (CMPs) for violations of the FCA, fraud charges, and even prison time.

Advancements in technology and AI are transforming risk adjustment workflows. Providers are increasingly relying on AI tools not only to assist with documenting patient visits through ambient listening, but also to identify potential diagnoses during patient encounters, while health plans leverage AI to manage chart reviews and respond to expanding CMS audit requirements. Even CMS is utilizing technology in chart reviews in their effort to address FWA in risk adjustment practices.[56] However, this technology



[56] "CMS Rolls Out Aggressive Strategy to Enhance and Accelerate Medicare Advantage Audits," Centers for Medicare & Medicaid Services (CMS), Press Release, August 2023: www.cms.gov/newsroom/press-releases/cms-rolls-out aggressive-strategy-enhance-and-accelerate-medicare-advantage-audits.

may misconstrue provider notes, miscategorize conditions and introduce bias and error propagation in the risk adjustment process. With robust governance and a human-in-the-loop approach, AI can reduce administrative burdens, advance clinical decision making, enhance quality by improving care management, and ensure accurate revenue, while boosting documentation accuracy and efficiency without compromising compliance.

The DOJ and HHS-OIG are actively investigating MA plans and providers for noncompliance in risk-adjustment processes, such as conducting one-way chart reviews (adding new codes but not removing unsupported ones), submitting diagnoses that aren't relevant to the visit or those identified in HRAs that were not reported on any other records of services, and generally investigating those failing to correct or disclose known coding errors. Whistleblower (qui tam) lawsuits and audit findings have revealed patterns of overbilling and documentation gaps. CMS estimates that MA plans may be overpaid by as much as $17 billion annually. In response, CMS has expanded its RADV audit program and is planning to conduct annual audits for every MA contract. CMS's RADV strategy includes increasing sample sizes from 35 to up to 200 per audit, conducting RADV audits for payment years 2018-2024 by 2026, and extrapolating findings to full contract populations.[57] However, with the recent vacation of the 2033 RADV final rule provisions, the applicability of CMS's extrapolation strategy is currently in question.[58]

The compliance burden is not limited to health plans. As value-based care models proliferate, provider organizations engaged in risk-sharing arrangements may also face financial exposure from identified overpayments. Providers with patterns of noncompliant coding may be subject to direct regulatory scrutiny, contractual penalties and reputational damage.

For chief compliance officers, this enforcement climate demands proactive governance. Organizations must implement robust internal controls, conduct regular coding audits and ensure that all diagnoses submitted for risk adjustment are clinically valid and properly documented. The message from regulators is unequivocal: accuracy is not optional.

[57] "CMS Rolls Out Aggressive Strategy to Enhance and Accelerate Medicare Advantage Audits," Centers for Medicare & Medicaid Services (CMS), Press Release, August 2023: www.cms.gov/newsroom/press-releases/cms-rolls-out-aggressive-strategy-enhance-and-accelerate-medicare-advantage-audits.

[58] "Judge Sides with Humana, Tosses Medicare Advantage Audit Rule," Becker's Payer Issues, September 26, 2025: www.beckerspayer.com/legal/judge-sides-with-humana-tosses-medicare-advantage-audit-rule/.

Compliance strategies for ensuring accurate risk adjustment

A well-structured compliance program is essential to minimizing risk adjustment vulnerabilities and ensuring regulatory alignment. Chief compliance officers play a critical role in establishing and maintaining the internal governance necessary to promote coding accuracy, including prevention mechanisms to detect anomalies early and remediating issues swiftly. Key compliance strategies include the following:

- **Foster a culture of compliance:** Establish and actively promote accessible channels for reporting potential misconduct, such as ethics hotlines and digital reporting platforms. These mechanisms should be clearly communicated across all levels of the organization to ensure visibility and ease of use. All reports of noncompliance must be subject to prompt, thorough and impartial investigation. Complainants should receive timely updates and respectful communication throughout the process to reinforce trust and demonstrate organizational commitment to integrity. Compliance departments should regularly analyze reported issues to identify patterns or emerging risks and implement corrective actions where necessary. Additionally, periodic enterprisewide education initiatives should be conducted to reinforce the importance of reporting, including the sharing of anonymized examples of successful issue resolution while reaffirming the organization's zero-tolerance stance on retaliation.
- **Establish rigorous policies and training protocols:** Enact clear, enforceable internal policies that mandate adherence to International Classification of Diseases, Tenth Revision (ICD-10) coding guidelines and CMS documentation standards. This includes ensuring that all submitted diagnoses meet CMS's "MEAT" criteria (Monitored, Evaluated, Assessed, or Treated) demonstrating that the condition is actively managed and clinically relevant. To support these policies, organizations must invest in ongoing

Compliance strategies at a glance

- Foster a culture of compliance
- Establish rigorous policies and training protocols
- Perform oversight of coding technologies and incentive structures
- Enforce two-way retrospective chart reviews
- Conduct auditing and monitoring for risk adjustment integrity
- Ensure prompt correction and incident response

education for both providers and coding professionals. Training should be conducted regularly and tailored to evolving regulatory expectations, audit findings and internal risk assessments. A structured feedback loop between coding teams and providers is essential to identify documentation gaps, address coding trends and reinforce best practices. Chief compliance officers should oversee the development and execution of these programs, ensuring that training is not only comprehensive but also measurable in its impact.

- **Perform oversight of coding technologies and incentive structures:** Implement governance protocols to ensure that any technology used in coding, particularly AI-driven suspecting tools or automated coding platforms, is subject to rigorous validation. This includes regular reviews of algorithms for accuracy, bias and compliance with CMS requirements and industry guidelines and ensuring that all AI-generated coding suggestions are reviewed and approved by qualified human coders prior to submission. Equally important is the evaluation of internal incentive structures, as incentive programs that reward coding volume, such as bonuses tied solely to the number of Hierarchical Condition Categories (HCCs) captured, may inadvertently encourage noncompliant behavior. Chief compliance officers should advocate for incentive models that prioritize quality, such as coding accuracy rates, documentation completeness and audit performance.
- **Enforce two-way retrospective chart reviews:** Adopt a two-way approach for conducting retrospective chart reviews to identify both diagnosis codes that were supported but not submitted and those that were submitted but lack sufficient documentation in the medical record. Chief compliance officers should ensure that review protocols include clear procedures for documenting unsupported diagnoses and submitting timely deletions to CMS. This process must be governed by internal controls that prioritize accuracy over revenue optimization. Two-way reviews demonstrate a commitment to ethical coding practices and regulatory compliance. Some organizations conduct concurrent or pre-bill audits, which allows auditors to query providers when the medical record documentation is not clear or diagnosis codes require clarification. Queries must be used compliantly in accordance with coding guidance, and processes must be put in place to ensure any queries do not impact timely claims submission.[59]

[59] "2022 ACDIS Practice Brief: Guidelines for Achieving a Compliant Query Practice," American Health Information Management Association (AHIMA), December 12, 2022: ahima.org/media/51ufzhgl/20221212_acdis_practice-brief.pdf.

- **Conduct auditing and monitoring for risk adjustment integrity:** Conduct periodic sample reviews to verify that all submitted diagnosis codes are fully supported by documentation in the medical record, including those derived from HRAs, which should also be corroborated by the member's treating providers. Advanced data analytics should be leveraged to identify coding anomalies such as outlier providers who consistently report high-severity conditions at rates significantly above their peers, or diagnoses that show unusual year-over-year increases. These insights can help pinpoint areas of potential noncompliance and guide targeted interventions. To further strengthen oversight, organizations should actively use the HHS-OIG's Medicare Part C High-Risk Diagnosis Codes Tool Kit to monitor frequently miscoded or unsupported diagnoses.[60] Performing routine internal mock RADV audits that simulate CMS's audit process can help organizations assess audit readiness and identify gaps before formal reviews occur. Audit findings should be systematically tracked and reported to senior leadership, the compliance committee and the board to ensure that risk adjustment remains a strategic priority and that necessary corrective actions receive executive support and resourcing.
- **Ensure prompt correction and incident response:** Correct or delete improper diagnoses from internal systems and refund any overpayments in accordance with the CMS overpayment rule. Under CMS's Final Rule, effective January 2025, the definition of "identified overpayment" has been clarified to trigger the 60-day repayment obligation.[61] The rule also introduces a 180-day suspension period to allow for a timely, good faith investigation into whether additional related overpayments exist. Chief compliance officers must ensure that internal procedures are aligned with these updated requirements and that documentation of all corrective actions is maintained. If systemic issues are uncovered, such as recurring documentation failures or coding inaccuracies,

[60] "Toolkit: To Help Decrease Improper Payments in Medicare Advantage Through the Identification of High-Risk Diagnosis Codes," U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG), December 14, 2023; oig.hhs.gov/reports/all/2023/toolkit-to-help-decrease-improper-payments-in-medicare-advantage-through-the-identification-of-high-risk-diagnosis-codes/.

[61] "Medicare and Medicaid Programs: CY 2025 Payment Policies Under the Physician Fee Schedule and Other Revisions to Part B," Federal Register, Vol. 89, No. 236, December 9, 2024: www.federalregister.gov/documents/2024/12/09/2024-25382/medicare-and-medicaid-programs-cy-2025-payment-policies-under-the-physician-fee-schedule-and-other#p-6100.

organizations should implement corrective action plans. These may include retraining specific personnel, revising internal workflows or initiating disciplinary measures. In cases involving significant risk or potential regulatory exposure, consultation with legal counsel regarding voluntary self-disclosure may be prudent as it can mitigate penalties and demonstrate a proactive compliance posture, especially when compared to enforcement initiated through whistleblower actions or DOJ investigations.

In today's heightened regulatory environment, precision in risk adjustment coding is not optional, it is a strategic and financial imperative. The convergence of substantial monetary incentives, rapid technological innovation and intensified federal oversight has positioned risk adjustment as a high-risk compliance domain. Chief compliance officers must lead with vigilance, ensuring that systems accurately reflect each member's clinical status and that all submissions are supported by robust documentation.

By implementing strong governance over emerging technologies, aligning internal policies with evolving CMS requirements, and fostering a culture rooted in accuracy and accountability, chief compliance officers can help their organizations navigate risk-adjusted payment models responsibly and reduce exposure to enforcement actions under the FCA. Moreover, by championing rigorous audit practices, proactive incident response and transparent reporting to executive leadership, Compliance departments play a critical role in protecting their organizations from legal exposure and reputational harm. This not only safeguards financial integrity but also contributes to a fairer, more effective healthcare system by ensuring that payments reflect true member needs and that compliance remains central to operational excellence.

Pharmacy benefit manager oversight

Pharmacy benefit managers are pivotal in managing prescription drug benefits for health plans, acting as intermediaries between health plans, pharmacies and drug manufacturers. Their responsibilities include negotiating drug prices, managing formularies, processing claims and administering rebates. While PBMs can help control drug costs and streamline pharmacy operations, their complex and often opaque business practices introduce significant compliance risks. As regulatory scrutiny intensifies and fiduciary obligations expand, Compliance departments must prioritize robust PBM oversight to safeguard participant interests and mitigate legal exposure.

A primary concern is lack of transparency. PBMs may engage in spread pricing (where PBMs charge health plans more for a drug than it pays the pharmacy), retain undisclosed rebates or charge hidden fees, obscuring the true cost of prescription drugs and undermining the health plan sponsor's ability to assess value. These practices can result in inflated costs for both plans and participants and may violate contractual or regulatory expectations.

Many PBM contracts lack clear definitions around pricing guarantees, rebate pass-throughs, and audit rights. Without precise language, health plans may struggle to enforce compliance or recover losses resulting from PBM misconduct. These gaps can also hinder the plan's ability to demonstrate fiduciary diligence in regulatory audits or participant disputes.

Federal and state reforms are increasingly targeting PBM practices, mandating greater transparency in rebate handling, pricing methodologies and pharmacy networks.[62] Compliance departments must stay informed of evolving legislation, such as the Consolidated Appropriations Act (CAA) and state-level PBM reform laws, which impose new disclosure and compliance requirements.[63]

Compliance strategies for PBM oversight

A well-structured compliance program is essential to minimizing PBM-related vulnerabilities and ensuring regulatory alignment. Chief compliance officers play a critical role in establishing and maintaining the governance necessary to promote transparency, detect anomalies early and remediate issues swiftly and effectively. Key compliance strategies include the following:

- **Conduct thorough due diligence:** Actively participate in the selection and renewal of PBM partnerships by conducting comprehensive evaluations of PBM compliance programs, fee structures, rebate arrangements and historical performance. This process should leverage third-party assessments where appropriate and ensure that compliance has a formal role in the review and approval process.
- **Ensure contract transparency and safeguards:** Partner with the Legal department and potentially leverage AI-based contract analysis tools to ensure that all PBM agreements contain explicit terms regarding pricing methodologies, rebate disclosures and favorable audit access. These provisions empower health plans to monitor PBM activities and enforce accountability through contractual rights.

Compliance strategies at a glance

- Conduct thorough due diligence
- Ensure contract transparency and safeguards
- Implement ongoing performance monitoring
- Effectuate regulatory change management
- Collaborate with regulators and PBM partners
- Retain documentation and evidence
- Promote compliant conduct

[62] "Fact Sheet: President Donald J. Trump Announces Actions to Lower Prescription Drug Prices," The White House, April 15, 2025: www.whitehouse.gov/fact-sheets/2025/04/fact-sheet-president-donald-j-trump-announces-actions-to-lower-prescription-drug-prices/.

[63] "Consolidated Appropriations Act, 2021 (CAA): Marketplace Oversight and Other Insurance Protections," Centers for Medicare & Medicaid Services (CMS), 2021: www.cms.gov/marketplace/about/oversight/other-insurance-protections/consolidated-appropriations-act-2021-caa.

- **Implement ongoing performance monitoring:** Implement robust data analytics and key performance indicators for key operational areas, especially member-facing activities such as coverage decisions to uncover discrepancies and ensure adherence to contractual and regulatory standards. Deploy AI-enabled reporting to identify trends of noncompliance to drive corrective actions and improve regulatory performance. Compliance and Delegation Oversight departments should conduct periodic audits to assess rebate flows, PBM compliance, cost effectiveness and alignment with member needs.
- **Effectuate regulatory change management:** Track federal and state PBM reform efforts, interpret their implications for the health plan and communicate updated expectations and requirements to PBM partners. Consider use of AI to identify new laws and reporting requirements and monitor member protections, and ensure timely updates to internal policies and PBM contracts.
- **Collaborate with regulators and PBM partners:** Engage proactively with state and federal agencies, as well as PBM partners, to clarify implementation timelines, data-sharing requirements and ambiguous regulations. Establish regular communication channels, participate in industry workgroups and document all regulatory guidance and partner communications to ensure transparency and readiness for regulatory review.
- **Retain documentation and evidence:** Document all activities related to PBM oversight, including contract reviews, audit findings and communications to support the Employee Retirement Income Security Act (ERISA) and CAA compliance and the plan's commitment to member wellbeing.
- **Promote compliant conduct:** Perform regular delegation oversight of PBMs and ensure that pharmacy-related requests are fully integrated into FWA identification and investigation processes. Additionally, Compliance departments should ensure that PBMs conduct robust drug management programs to identify those members at risk for misuse or abuse of drugs. PBMs should take action to restrict at-risk members to utilize designated prescribers and pharmacies when necessary, and should share program results with the health plan regularly. Accessible and well-publicized

reporting mechanisms must be established, enabling both health plan and PBM staff to report suspected misconduct confidentially. All reports of noncompliance should be investigated promptly, thoroughly and impartially, with outcomes documented and tracked. Compliance departments should analyze reported issues to identify trends or emerging risks and implement corrective actions as needed. Periodic, enterprisewide education initiatives should reinforce the importance of reporting concerns and share anonymized examples of successful issue resolution to foster a culture of transparency and accountability.

PBM oversight is no longer a peripheral concern, but rather a core compliance function. Health plans should evaluate their current PBM oversight frameworks and take immediate steps to align with emerging regulatory standards and industry expectations. As regulatory expectations rise and standards tighten, health plans must cultivate strategic, transparent and accountable relationships with their PBMs. By doing so, they protect their members, fulfill their legal obligations, and position themselves for long-term success in a complex and fast-changing healthcare system.

As regulatory scrutiny intensifies and fiduciary obligations expand, Compliance departments must prioritize robust PBM oversight to safeguard participant interests and mitigate legal exposure.

Encounter management

Effective health plan encounter management is critical for chief compliance officers because it ensures accurate reimbursement, regulatory compliance, risk adjustment integrity, FWA prevention and reliable quality reporting, while providing a strong foundation for audit readiness and organizational integrity. Accurate and timely encounter submissions are a critical focus for federal and state regulators, as they serve as a primary mechanism for evaluating whether health plan members are receiving appropriate and necessary care with expected outcomes. Regulators and health plans rely on this data to monitor service utilization, assess quality care standards, identify potential FWA and ensure that managed care organization contractual obligations are fulfilled. Encounter data also plays a central role in determining payments to health plans, as it informs rate setting and risk adjustment payments. Additionally, encounter data received from delegated providers is a vital input in member explanations of benefits (EOBs), driving appeal rights and impacting access to care.

Encounter creation often leverages applications that create encounters based on adjudicated claims. When encounters are unable to meet submission requirements, manual processes are often required to resolve the identified issues. Given the constant flow of adjudicated claims, impacted parties quickly become inundated with growing backlogs that may impact the timeliness of encounter submissions. Incomplete or inaccurate encounter submissions can result in reduced reimbursement, increased regulatory scrutiny and negative impacts to member access to care.

Compliance strategies for encounter management

Effective encounter management is essential to reduce compliance risks and ensure regulatory alignment for health plans, as encounters sit at the crossroads of compliance, operations and financial performance. Chief compliance officers, in partnership with operational leaders, play a critical role in maintaining accurate, timely encounter submissions that support reimbursement integrity, risk adjustment accuracy and FWA prevention. Robust processes enable transparency, facilitate early detection of anomalies and safeguard audit readiness while mitigating the financial and operational impacts of incomplete or delayed data. By prioritizing encounter accuracy and timeliness, organizations strengthen their ability to meet contractual obligations, uphold member access to care and maintain organizational integrity. Key compliance strategies include the following:

- **Evaluate internal encounter controls:** Conduct a formal evaluation of internal controls across the encounter data lifecycle. Ensure controls are documented, tested regularly and aligned with CMS and state-specific requirements. Collaborate with IT and operations to implement automated validations and audit trails.
- **Analyze rejected encounters:** Evaluate implementation of AI solutions to identify trends in encounter rejections. Facilitate cross-functional engagement with claims, IT and operations to analyze identified trends, document root causes and support the implementation of upstream process improvements, including predictive analytics for future encounter submissions. Monitor resolution timelines and ensure corrective actions are tracked.
- **Review manual intervention and pended encounter management:** Request an inventory of all manual interventions used to address pended (cannot be processed) encounters and assess their effectiveness

Compliance strategies at a glance

- Evaluate internal encounter controls
- Analyze rejected encounters
- Review manual intervention and pended encounter management
- Examine encounter reporting
- Implement encounter governance and cross-functional collaboration
- Ensure timely submission of delegate encounters
- Assess encounter vendor oversight

and sustainability. Partner with operations to develop long-term automation strategies, eliminate recurring pending encounters and ensure documentation supports audit readiness.

- **Examine encounter reporting:** Review KPIs and exception reports related to encounter submissions. If reporting is insufficient, collaborate with Data Science or IT departments to develop dashboards that highlight timeliness, accuracy and rejection rates. Use these insights to inform compliance risk assessments.
- **Implement encounter governance and cross-functional collaboration:** Advocate for integrating encounter submission requirements into the claim ingestion and adjudication processes. This proactive approach reduces downstream errors and regulatory scrutiny. Moreover, routine communication between compliance, claims, encounters and network management fosters a preventive culture by enabling early identification of risks and promoting shared accountability for data integrity.
- **Ensure timely submission of delegate encounters:** Establish formal oversight mechanisms to monitor the quality and timeliness of encounter submissions by delegated providers, including routine audits and data-integrity attestations, as well as reviewing performance against contractual obligations. Compliance departments should also collaborate with operational teams to define clear escalation paths for unresolved issues and ensure that delegates receive ongoing guidance on regulatory expectations.
- **Assess encounter vendor oversight:** Evaluate vendor reliance in encounter data processing and review monitoring protocols used by business owners to ensure they include performance metrics, issue tracking and remediation timelines. Compliance departments should also periodically audit vendor adherence to contractual and regulatory obligations, potentially through delegation oversight functions.

Incomplete or inaccurate submissions of encounter data can lead to serious consequences, including reduced reimbursement, increased oversight and compromised member access to care. By proactively evaluating internal controls, monitoring vendor performance and fostering cross-functional collaboration, chief compliance officers can help ensure that encounter data meets regulatory standards and supports organizational goals. Integrating encounter requirements into upstream processes like claims adjudication is essential to reducing downstream issues. Ultimately, a strong compliance framework around encounter data not only mitigates risk but also reinforces the health plan's commitment to delivering appropriate, timely and high-quality care.

In closing

As healthcare organizations contend with a rapidly shifting regulatory landscape, the imperative for a robust, adaptive and effective compliance program is clearer than ever. The seven foundational elements of an effective compliance program are not just requirements, but strategic pillars for navigating complex federal and state mandates, heightened enforcement and operational uncertainty.

Yet, the execution of these programs is increasingly challenged by significant staffing constraints. Many Compliance departments are facing workforce reductions or stagnant headcounts, even as their responsibilities expand. The proliferation of new regulations, regulatory focus on FWA, increased use of vendors and delegated entities requiring oversight, and the need to respond to frequent audits have placed unprecedented demands on Compliance departments. Often, staffing levels are not scaled to match these growing obligations, resulting in gaps in oversight, delayed issue resolution and diminished capacity for proactive risk management.

Compounding these pressures is the difficulty in attracting and retaining qualified compliance professionals. The demand for specialized expertise in areas such as privacy, security, risk adjustment and vendor oversight far outpaces supply, leaving many organizations unable to fill critical roles. Without adequate staffing, even the most well-designed compliance frameworks may falter, exposing organizations to regulatory findings, financial penalties and reputational harm.

To address these mounting challenges, organizations are increasingly leveraging both external subject-matter expertise and advanced technologies to enhance their compliance processes to ensure their compliance programs remain resilient and responsive to new regulatory demands, even amid workforce constraints.

At the same time, automation and AI are transforming the way Compliance departments operate. Automation can efficiently handle routine tasks such as monitoring adherence to policies, conducting risk assessments and managing documentation, freeing up valuable staff time for more strategic and analytical work. AI-powered analytics go a step further by sifting through vast amounts of data to identify patterns, anomalies or emerging risks that may indicate compliance issues or potential security threats. By integrating these technologies, health plans can significantly reduce the administrative burden on their Compliance departments, allowing professionals to focus on initiatives that drive innovation, strengthen internal governance and enhance member trust.

It is incumbent upon chief compliance officers to lead with integrity, vision and purpose, fostering a culture where ethical conduct and accountability are paramount. By championing robust compliance programs, anticipating and mitigating risks, and guiding their organizations through complexity, they empower organizations, protect members and drive sustainable success. Through their leadership, chief compliance officers turn challenges into opportunities, ensuring that organizational values and compliance excellence remain at the forefront of every decision.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI).

About Protiviti's healthcare industry practice

At Protiviti, we know healthcare. Our global reach continues to expand at a rapid pace as we serve leading healthcare organizations amid accelerating change. We know the industry changes that are imminent and their drivers. And we know how to advise our clients to effectively address industry changes to best manage, protect and create substantial value. Our team of experienced professionals and our Healthcare Center of Excellence are your resources for understanding and managing the multitude of changes and risks affecting healthcare. Whether your organization's chief concern is payment reform, regulatory compliance, revenue growth, cost management, cybersecurity, technology modernization or adoption of AI, Protiviti is here for you.

About the authors

Leyla Erkan

Managing Director, Global Healthcare Legal, Risk & Compliance Practice Leader

Leyla is Protiviti's Global Healthcare Legal, Risk & Compliance Practice Leader. She brings over 25 years of expertise in compliance and risk management, including a distinguished career as a Chief Compliance, Privacy and Research Officer. Leyla has deep expertise in regulatory compliance, clinical research, privacy, conflicts of interest, investigations and government audits, offering a comprehensive understanding of and practical approach to complex healthcare challenges. She can be reached at leyla.erkan@protiviti.com.

Megan Allison

Associate Director, Global Healthcare Legal, Risk & Compliance Payer Practice Leader

Megan is Protiviti's Global Healthcare Legal, Risk & Compliance Payer Practice Leader, with more than 20 years of expertise in compliance and risk management across the healthcare landscape, including serving in senior leadership roles across Medicare Advantage, Medicaid Plans, Clinically Integrated Networks, and Provider Health Systems. Megan has extensive expertise in regulatory compliance, audit readiness, CMS program audits, delegation oversight, and risk adjustment strategy, delivering strategic and actionable solutions to the most intricate compliance challenges. She can be reached at megan.allison@protiviti.com.

11,000+	90+	25+	$2 BN
Protiviti professionals*	office locations worldwide	countries	in revenue*

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA*
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®