Key Takeaways: 7th Annual "Let's Talk Compliance" Conference

04 March 2025

Editor's Note: PYA and Foley & Lardner hosted the 7th Annual "Let's Talk Compliance" two-day virtual conference on January 23 and 24, 2025. Panelists included Foley attorneys and PYA subject matter experts. The event was hosted by Foley partner, Jana Kolarik, and PYA consulting principal, Angie Caldwell. Below are key takeaways from each session. The recorded sessions and PowerPoints can be accessed here.

Session 1: The OIG's General Compliance Program Guidance: "Auld Lang Syne"

Foley Partner Judy Waltz, Chair of Foley's Health Care Practice Group, and PYA Consulting Principal Shannon Sumner kicked off the 2025 series of "Let's Talk Compliance" presentations with updates on health care compliance expectations and enforcement.

The Trump Administration has confirmed by recent actions and comments that identifying fraud, waste, and abuse (collectively referenced below as "fraud") in the Medicare and Medicaid programs will continue to be a top enforcement priority. See e.g., NPR's article "DOGE sets its sights on Medicare and Medicaid." Early actions from the Department of Government Efficiency (DOGE) suggest an increased focus on datamining to identify suspected fraud.

In light of expected continued or increased scrutiny, providers and suppliers should continue to focus on assuring their compliance programs are (and can be demonstrated to be) effective at avoiding and responding to operational fraud. Even in the event of a compliance oversight failure, having an otherwise effective compliance program can help providers mitigate ensuing damages alleged as fraud.

OIG's GCPG. Sumner started the discussion with a recap and update of the U.S. Department of Health and Human Services (HHS) Office of Inspector General (OIG) General Compliance Program Guidance (GCPG), issued in November 2023. The basics of the GCPG were discussed in last year's session, and a summary can be found here. Importantly, compliance with the GCPG is voluntary.

In this year's session, titled "The OIG's General Compliance Program Guidance: "Auld Lang Syne,"" Waltz and Sumner shared their observations one year after the GCPG was released. The following highlights were noted.

Quality Review and Integration With Compliance. As discussed in the GCPG, Waltz and Sumner recommended the integration of compliance with quality, including an increased engagement with and collaboration between compliance and quality committees. In this context, Sumner highlighted the importance of the compliance officer meeting with the board of directors at least quarterly and the need for effective risk assessment evaluation. She emphasized the importance of training and education, including methods for attendees to ask questions, and the consideration of “mini” training modules. She highlighted the importance of regular reports to the board of directors from senior leadership on quality and patient safety.

State Exclusions. Waltz reminded attendees of the GCPG’s emphasis on the need for state Medicaid exclusion checks in addition to a review of the federal exclusion lists. She also noted that states appeared to be increasing their collateral exclusion actions taken against their own Medicaid providers as a result of exclusion actions taken in another state, as required by the Affordable Care Act and implementing regulations.

Best Practices. The following “best practices” were identified for GCPG implementation that may be generally applicable to all industry segments.

Greater awareness by facility governance regarding appropriate reporting relationships (e.g., compliance officer reporting directly to the CEO with independent access/reporting to the board directly and NOT reporting to legal).

Greater *demonstrated* engagement by the Compliance Committee(s) – at the Board level and entity level.

Active engagement by the Compliance Committee in overseeing/participating in the risk assessment process.

Various multi-disciplinary committees with active compliance involvement – Enterprise Risk Management (ERM), quality, root cause analysis, data governance, artificial intelligence, change management.

Vendor/third-party risk assessment and mitigation awareness has increased.

Governance (Board/Board subcommittee) must have greater awareness of compliance program oversight and accountability.

Need for creative compliance training curriculums and delivery mechanisms.

Key compliance controls with inventory by department.

OIG’s Nursing Facility ICPG. Following last year’s GCPG, OIG issued its first ICPG in November 2024. OIG anticipates a series of these segment-specific guidance documents to address at least Medicare Advantage plans, hospitals, hospice, clinical laboratories, and pharmaceutical manufacturers. Like the GCPG, this ICPG is filled with helpful references and links that make for easy review. Because this ICPG was directed at a limited business segment, Sumner and Waltz did not discuss it in detail but rather focused on its structure and organization as predicting how future ICPGs will look.

One theme that carried through to this ICPG from the GCPG was OIG’s focus on quality of care. OIG made frequent references to the nursing facility requirements of participation and to OIG’s experience with quality-of-care Corporate Integrity Agreements (CIAs). Among the areas suggested for review in the nursing facility setting were appropriate use of medications, resident safety, staff screening, and avoiding billing for excluded providers. OIG also underscored its expectations that “investors” [in addition to other categories of managing and controlling entities or individuals] will have a continuing focus on compliance and quality.

Steps to Take Now. Although HHS’ staff has been reduced, and enforcement in certain other regulated areas may no longer be an area of priority, as yet there has been no suggestion that the Trump Administration will reverse years of OIG focus on reducing fraud, waste, and abuse in the Medicare and Medicaid programs. To the contrary, the Trump Administration seems to be counting on savings from stopping identified fraud to fund other priorities. Providers and suppliers should continue to invest in and critically evaluate the performance of their corporate compliance programs. The GCPG provides specific guidance for assessing compliance program effectiveness across health care industry sectors, while the ICPGs will provide more direct guidance based on sector segment.

Session 2: Trends in Health Care Privacy and Security: Cybersecurity, Patient Rights, and Reproductive Health Care Information.

Foley partner Jennifer Hennessy and PYA principal Barry Mathis provided a refresher on HIPAA’s right for individuals to access their own information and discussed HIPAA’s reproductive health care information amendments, the proposed updates to the HIPAA Security Rule, the Security Risk Analysis Enforcement Initiative, and recent ransomware settlements. They also discussed effective strategies for cyber event response, artificial intelligence (AI), and tips for managing cyber risks with third-party vendors.

Hennessy emphasized the importance of understanding HIPAA’s access requirements, including the 30-day response timeframe, the requirement to provide all protected health information (PHI) in the designated record set, and the limitations on fees. Understanding and complying with these requirements is key in light of U.S. Department Health and Human Services’ (HHS) HIPAA Right to Access Initiative, now with over 50 settlements.

Hennessy also addressed the HIPAA amendments protecting reproductive health care information and emphasized the need for HIPAA-regulated entities to obtain an attestation before disclosing reproductive health care information to health oversight agencies, law enforcement, or coroners or medical examiners, or in judicial or administrative proceedings. She also discussed the pending lawsuits challenging these amendments and the potential that the Trump Administration may not enforce the amendments, although that is still unclear at this time.

The presenters then turned to cybersecurity, including HHS’ proposed updates to the HIPAA Security Rule to safeguard electronic PHI from cybersecurity threats. The proposed updates include eliminating the distinction between required and addressable implementation specifications, requiring a written inventory of technology assets, and more stringent requirements for an annual security risk analysis, among other proposals. Comments to the proposed rule are due by March 7, 2025.

Continuing its enhanced focus on cybersecurity, HHS has announced a Security Risk Analysis Enforcement Initiative, to focus select investigations on compliance with the HIPAA Security Rule Risk Analysis provision. HHS issued its first settlement under the initiative in October 2024, related to a ransomware attack. The presenters noted that the key takeaway from the initiative is that organizations should ensure they have an up-to-date and thorough risk analysis, as well as a risk management plan where identified risks and vulnerabilities are remediated in a timely manner.

Mathis underscored the critical need for robust cybersecurity measures, including a comprehensive response plan, continuous monitoring, and the use of AI for advanced threat detection. He advocated for storing data securely in the cloud and stressed the importance of strict monitoring and security requirements for third-party vendors to safeguard against sophisticated data exfiltration techniques employed by malicious actors.

Mathis emphasized the following general key recommendations for actions that providers can take:

- Conduct a security risk analysis of the potential risks and vulnerabilities to electronic PHI and update it regularly.
- Ensure privacy and security policies address HIPAA’s requirements.
- Implement strong security controls such as Multi-Factor Authentication.
- Keep systems updated.
- Implement security procedures to comply with the HIPAA Security Rule and other cybersecurity frameworks (e.g., review information system activity).

Train workforce members on cybersecurity and HIPAA policies and procedures.

Develop and test cyber incident response scenarios.

Session 3: A New Era for Interacting with Federal Agencies

Foley partner Matthew Krueger and PYA principal Martie Ross addressed how the end of *Chevron* deference to agency interpretations in implementing statutory directives, and the reelection of President Trump, will impact the work of federal agencies like the Department of Health & Human Services and its component, the Centers for Medicare & Medicaid Services (CMS). Both Krueger and Ross recommended that organizations actively monitor challenges to regulations because courts are more likely to enjoin or invalidate regulations in light of the Supreme Court’s decision in *Loper Bright* overturning *Chevron*.

They also identified that this new era may create opportunities to challenge regulations or subregulatory guidance (e.g., Medicare manuals or contractor guidance) that exceeds an agency’s underlying statutory authority, whether through a rulemaking challenge or in response to enforcement actions. They also encouraged organizations to consider these developments when developing internal risk assessments and to recalibrate risk in light of *Loper Bright* and the Trump Administration.

Session 4: Antitrust Issues in Provider Mergers and Acquisitions

Foley partner Ben Dryden, vice-chair of Foley’s Antitrust & Competition Practice Group, and PYA principal Michael Ramey discussed the antitrust issues that come up in mergers and acquisitions involving health care providers. They discussed recent antitrust enforcement trends, the 2023 revisions to the federal *Merger Guidelines*, and the upcoming changes to the rules for reporting large transactions under the Hart-Scott-Rodino Act.

In the area of compliance, Dryden and Ramey discussed the need to develop protocols for sharing competitively sensitive information in due diligence and integration planning, including using a “clean team” or “black box” approach where appropriate. They also discussed the increasing role that state regulators are playing in health care merger reviews, including laws in several states that require premerger notifications to state regulators, and “Certificate of Public Advantage” laws that, in certain cases, can immunize a transaction from federal antitrust scrutiny. They ended with a discussion of the likely enforcement priorities of the Trump Administration, including an increased focus on consumer impacts and a possible softening of skepticism towards private equity investments in health care.

Stay Connected

For more information on our “Let’s Talk Compliance” insights, subscribe to our “Let’s Talk Compliance” blog and podcast series. Please reach out to Jennifer or Barry if you have any

questions on the topics covered in this session of the Let’s Talk Compliance annual event.

Author(s)

Judith A. Waltz
Partner

Jennifer J. Hennessy
Partner

Matthew D. Krueger
Partner

Benjamin R. Dryden
Partner

View More