COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 33, Number 35. September 30, 2024
Updated DOJ Compliance Guidance Adds AI; 'If You're Not Doing These Things, Why Not?'

By Nina Youngstrom

Whether organizations consider all the angles of artificial intelligence (AI) and other technology is a new focus of the fourth update to guidance on effective compliance programs from the U.S. Department of Justice (DOJ).[1] Internal whistleblowing and nonretaliation also get a higher profile in the latest version of the *Evaluation of Corporate Compliance Programs*, released Sept. 23.

"They clearly want to see compliance programs that are in the 21st century," said former federal prosecutor Anthony Burba with Barnes & Thornburg LLP in Chicago.

The guidance is used by white-collar prosecutors who evaluate compliance programs when deciding whether to file fraud charges and what the charges should be. Compliance officers also use the guidance to benchmark their organization's compliance program.

"Prosecutors will consider whether the company is vulnerable to criminal schemes enabled by new technology, such as false approvals and documentation generated by AI," said Nicole Argentieri, principal deputy attorney general, who announced the update during a speech at SCCE's Compliance and Ethics Institute in Grapevine, Texas Sept. 23.[2] "If so, we will consider whether compliance controls and tools are in place to identify and mitigate those risks, such as tools to confirm the accuracy or reliability of data used by the business."

The *Evaluation of Corporate Compliance Programs* shows how much DOJ is counting on organizations to self-police. "The government's take is the compliance officer's role and compliance program's role in the organization is ever expanding and is a critical element in detecting wrongdoing," said Carolynn Jones, chief compliance and risk officer at Harris Health in Texas. Compliance officers should review the guidance and "ask yourself, if you're not doing these things, why not, and how you might incorporate them into your program."

The guidance, which first came out in 2017, is organized around three "fundamental questions" that prosecutors try to answer when evaluating effectiveness:

1. "Is the corporation's compliance program well designed?"
2. "Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?"
3. "Does the compliance program work in practice?"

The rest of the guidance drills down into risk assessments, commitment by senior and middle management, confidential reporting, resources and other compliance classics, as well as related issues, such as due diligence for mergers and acquisitions. The 2024 version has new or amplified sections on technology, whistleblowers and data. "We have also updated the [guidance] to expand upon an important concept—that companies should be learning lessons from both the company's own prior misconduct and from issues at other companies to update

their compliance programs and train employees," Argentieri said.

But keep in mind the operative word is guidance. These aren't requirements for an effective compliance program and organizations should "think about how to right-size it," said attorney Matthew Krueger, with Foley & Lardner LLP. "The question is, what is a reasonable compliance program for your particular organization, taking into account its size and activities. DOJ will not expect an organization with two hospitals to have the same compliance program as a 20-hospital system," said Krueger, a former U.S. attorney.

DOJ Has Many Questions About AI Risk, Mitigation

A lot of ink is spilled on AI and other technology. It's under an existing section about prosecutors giving credit for "the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction." Here are a few of DOJ's risk-assessment type questions on technology, including AI: "How is the company curbing any potential negative or unintended consequences resulting from the use of technologies, both in its commercial business and in its compliance program? How is the company mitigating the potential for deliberate or reckless misuse of technologies, including by company insiders? To the extent that the company uses AI and similar technologies in its business or as part of its compliance program, are controls in place to monitor and ensure its trustworthiness, reliability, and use in compliance with applicable law and the company's code of conduct? What baseline of human decision-making is used to assess AI?"

That's a lot to wrap your head around, Jones said. AI is very broad and "it's popping up in all aspects of the business," from helping clinicians write a clinical note in the medical records to screening resumes from job applicants. Organizations need a governance structure to review AI tools one by one.[3] "From a compliance perspective, it's those initial questions [in the DOJ guidance] that compliance officers should be asking the executive team," Jones said. "At some point, it becomes part of your regular risk assessment process where you're interviewing department by department and asking how they use AI."

'DOJ Doesn't Want Legal Lording Over Compliance'

The second addition to the guidance centers on data. A compliance program will be judged partly on whether compliance officers have access to data and their organizations leverage data analytics "to create compliance efficiencies." Questions DOJ will ask include "How is the company measuring the accuracy, precision, or recall of any data analytics models it is using?"

Burba thinks the two most notable sections of the guidance are about the use of AI and data. "You need to be tracking your data to be running analytics," he said. "This continues to drive home the point that DOJ doesn't want legal lording over compliance. They want companies to be able to show their work. It's not just, 'Can you tell us about your program?' It's, 'Show us the receipts.'" What kicked off an internal investigation? What were the findings and how were they remediated? How was the whistleblower treated compared to the people responsible for the misconduct? "Traditionally, there's a reflex" to bring in the legal department "as soon as something becomes sensitive," Burba said. "Companies will be hamstringing themselves under" the DOJ guidance and its other recent policies, including the corporate enforcement policy, if they take that route.

There's a rich supply of data for compliance officers to tap into, such as claims data and the CMS Open Payments program. Software tools also are available to track and trend data. For example, Harris Health uses software to check the home addresses of employees who access medical records against the addresses of patients whose medical records were accessed. If the addresses are the same (i.e., a family member) or similar (i.e., a neighbor), it might indicate improper access. "There are different ways you can look for wrongdoing using data," Jones noted.

Drawing Out Internal Whistleblowers

The third addition to the DOJ guidance is about whistleblowing. Under the section on confidential reporting, DOJ added questions to test its effectiveness: "Does the company encourage and incentivize reporting of potential misconduct or violation of company policy? Conversely, does the company use practices that tend to chill such reporting? How does the company assess employees' willingness to report misconduct?" The same goes for nonretaliation policies. Among the new questions: "Does the company train employees on both internal anti-retaliation policies and external anti-retaliation and whistleblower protection laws?"

DOJ's emphasis on whistleblowers dovetails with its new corporate whistleblower awards program and the HHS Office of Inspector General's November 2023 *General Compliance Program Guidance*, Jones said. With DOJ shouting it from the rooftops, compliance professionals should consider creative new ways to be available to employees. "We're considering monthly office hours or a town hall where the compliance officer or team is on a Zoom call for a set hour and workforce members can dial in," she said. After talking about a compliance topic, the team will open the floor to questions. Harris Health also will be ramping up activities around Compliance and Ethics Week in November. "Every year, it gets a little bit bigger," Jones noted.

Although the corporate whistleblower awards program offers people money for information about certain types of fraud, DOJ is pushing whistleblowers to report it to the company first, Krueger said. "Making an internal report to the company before going to DOJ is a factor that will increase the amount of the whistleblower award," he noted. DOJ would prefer if companies nip problems in the bud before an enforcement action is inevitable. But prospects for that are dim if whistleblower rumblings never make it to compliance (e.g., reporting mechanisms are ineffective or employees are unconvinced by nonretaliation promises), Krueger said. That's why compliance officers should hammer home to leadership to send even a hint of a complaint their way. "There's more incentive for people to be whistleblowers now" between the False Claims Act and the new whistleblower awards program, he noted.

Contact Jones at carolynn.jones@harrishealth.org, Krueger at mkrueger@foley.com and Burba at tony.burba@btlaw.com.

1 U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated September 2024, https://bit.ly/3MXjYcK.
2 U.S. Department of Justice, Office of Public Affairs, "Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute," speech, September 23, 2024, Grapevine, Texas, https://bit.ly/3ZGJFGa.
3 Nina Youngstrom, "AI Governance Committee Work is Underway; Employee Use of Tools Is Monitored," *Report on Medicare Compliance* 33, no. 28 (August 5, 2024), https://bit.ly/4dlss8k.