COZEN
O'CONNOR

Avoiding FCA Scrutiny while Reaping the Benefits of AI

Companies are racing to harness the power of artificial intelligence. The applications are myriad. Insurers are using AI to replace administrative overhead and assist with claims processing. Software developers are incorporating AI to add value to their enterprise products. Even law firms are dipping their toes in the water, leaning into AI for research and writing, client correspondence, and document review.

But in the race to stay competitive, companies must also be careful to avoid pitfalls that could expose the company to civil and criminal penalties. Every company using AI should be aware of risks related to cybersecurity, confidentiality, and contractual requirements, as those issues have been widely covered. What companies may not appreciate at this stage, is that they could also face exposure under the False Claims Act (FCA) if their clients include Government agencies or contracts.

To date, most federal enforcement actions involving AI have fit squarely in the FCA's traditional use: allegations that a contractor misrepresented the product it sold to the Government. In these cases, AI is part of the software or technology product sold to the Government – usually for military defense or espionage purposes – but the legal theory supporting the claims are traditional. Nonetheless, these cases are a stark reminder that while some executives may consider misleading statements about their software's capabilities to be ambitious advertising, the Government could later cast those representations as fraud against the Government.

It is nearly certain, however, that the Government's scope of enforcement will extend beyond traditional FCA cases involving AI products. In September, the Department of Justice announced an update to its Evaluation of Corporate Compliance Programs (ECCP). This guidance is used by federal prosecutors to determine the effectiveness of a corporation's compliance program at the time of an offense and can impact resolution, monetary penalties, and imposed compliance obligations. New in September, the guidance specifically called for an analysis of how corporations manage AI. This analysis may inquire into the following:

- Is management of risks related to use of AI and other new technologies integrated into broader enterprise risk management strategies?
- 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?
- Do controls exist to ensure that the technology is used only for its intended purposes?
- What baseline of human decision making is used to assess AI?
- How is accountability over the use of AI monitored and enforced?

The ECCP is a clear signal from the Department of Justice that corporate AI programs are under scrutiny. Where companies fail to follow the Government's guidance and those failures result in the submission of false claims, companies should expect scrutiny and potential enforcement actions from the Government.

Indeed, the heightened scrutiny signaled by the ECCP has already commenced. The Government has pursued enforcement actions against health care providers who use algorithms or AI to suggest diagnosis codes or treatments and those suggestions result in medically unnecessary

Arthur P. Fritzinger

Member

afritzinger@cozen.com
Phone: (215) 665-7264
Fax: (215) 665-2013

Calli Jo Padilla

**Member
Co-Chair, Women's Initiative**

cpadilla@cozen.com
Phone: (215) 665-6938
Fax: (215) 253-6777

James Mahady

Associate

jmahady@cozen.com
Phone: (215) 701-2208
Fax: (215) 665-2013

Related Practice Areas
- White Collar Defense & Investigations

claims submitted to Medicare or Medicaid. The Government's somewhat novel theory – that false claims can result from inaccurate suggestions made by algorithms or other software, despite the intervening medical judgment of a physician – has been accepted by one district court in United States ex rel. *Osinek v. Permanente Medical Group*, 640 F. Supp. 3d 885 (N.D. Cal., 2022) but has otherwise avoided judicial scrutiny.

Other medical providers have run afoul of regulators by using AI to suggest diagnostic codes later determined to be improper, and by failing to follow suggestions of AI software when it encouraged revisiting prior diagnoses. In essence, the Government expects companies will use AI to reduce the monetary value of Medicare claims when appropriate, but may demand companies avoid following advice from AI if it results in higher bills to the Government. As AI becomes further integrated into medical practices, work flows and electronic health records, companies must be extremely careful to avoid any suggestion that the software has improperly influenced the medical judgment of treating physicians.

Finally, it is important to remember that the Government also uses AI to find fraud. As the Government relies more upon algorithms and data to identify potential violations, companies should be mindful of the biases in those programs. Certain innocuous behavior may be misidentified as suspicious by algorithms focused on the wrong data points. Those inaccurate algorithms may give regulators false confidence in cases that have little merit. And the costs of proving that will likely fall on companies themselves.

It is no secret that AI is here to stay. It creates powerful levers in the economic marketplace – that power can produce profits, but it comes with a liability risk. Companies should carefully consider the risks of implementing AI products if they have any government contracts or revenue sources. Ensuring, at the outset, that AI products are implemented subject to controls like those recommended by the ECCP can help avoid the costs and burden of subsequent Government scrutiny.