November 10, 2021

DOJ Civil Cyber-Fraud Initiative May Impact Health Care and Life Sciences Companies

Introduction

Attorneys
Deborah L. Gersh
Christine Moundas
Andrew O'Connor
Jamie E. Darch
Gregory Hardy

Deputy Attorney General Lisa O. Monaco recently announced a Civil Cyber-Fraud Initiative by the Department of Justice (DOJ) targeting companies that fail to meet government cybersecurity standards.[1] Under the initiative, DOJ's Civil Division's Commercial Litigation branch plans to utilize the False Claims Act (FCA) to pursue government contractors and grant recipients for misrepresenting their cybersecurity practices or falling short of the government's cybersecurity standards. After Monaco's announcement, Acting Assistant Attorney General Brian M. Boynton explained that the new initiative will focus specifically on at least three areas of accountability: failing to comply with cybersecurity standards, misrepresentation of security controls and practices, and failing to timely report suspected breaches.[2]

Although the announcement did not single out the health care industry, health care and life sciences companies should heed DOJ's announcement, which promises increased attention from both DOJ and the FCA relators' bar. Below we offer an overview of the initiative and steps companies can take now to mitigate their risk.

Implications for the Health Care Industry

According to Monaco, the initiative will target government contractors and federal grant recipients. Therefore, health care and life sciences companies that contract with, or receive grants from, the federal government may be subject to FCA scrutiny under the new initiative. For example, DOJ may begin scrutinizing academic medical centers (AMCs) or private health care companies that receive research grants for misrepresenting their cybersecurity practices in grant applications or reports, or for failing to comply with relevant reporting obligations—including disclosing data breaches.[3] While the intended scope of this initiative is not yet clear, it may apply to health care and life sciences companies that contract to provide services or products to the federal government (e.g., companies that contract with the Veterans Administration and/or participate in the Federal Supply Schedule).

While DOJ's announcement does not directly reference the cybersecurity standards to which the government expects organizations to comply, in August 2021 the Biden Administration called for the National Institute of Standards and Technology (NIST) to collaborate with industry and other partners to develop a new framework to improve the security

---

[1] Press Release, Department of Justice, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative* (Oct. 3, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[2] Remarks of Acting Assistant Attorney General Brian M. Boynton at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit (Oct. 13, 2021), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and.

[3] This initiative would not be the first time DOJ has targeted grant recipients in the AMC and health care space. For example, in 2019, Duke University paid the government $112.5 million to resolve FCA allegations that it submitted grant applications and progress reports to the NIH that contained false statements concerning the validity of its research. Press Release, Department of Justice, *Duke University Agrees to Pay U.S. $112.5 Million to Settle False Claims Act Allegations Related to Scientific Research Misconduct* (Mar. 25, 2019), https://www.justice.gov/opa/pr/duke-university-agrees-pay-us-1125-million-settle-false-claims-act-allegations-related. Similarly, in 2016, the United States District Court for the Eastern District of Kentucky found LifeTechniques, Inc. and Care Team Solutions LLC liable for $4.5 million for "making false statements" on NIH grant applications "about their personnel, facilities, and accounting systems." Press Release, Department of Justice, *U.S. District Court Orders $4.5 Million Civil Judgment Against Lexington Woman And Her Medical Device Companies For Committing Grant Fraud* (July 13, 2016), https://www.justice.gov/usao-edky/pr/us-district-court-orders-45-million-civil-judgment-against-lexington-woman-and-her.

and integrity of the technology supply chain.[4] Notably, NIST's existing cybersecurity framework has already been leveraged by the federal government to evaluate the cybersecurity practices of health care providers and organizations that are subject to the Health Insurance Portability and Accountability Act, as amended (HIPAA).[5] As a result, the current NIST cybersecurity framework and other existing frameworks may provide helpful guidance to health care organizations regarding the government's current expectations with respect to cybersecurity standards, and the evolution of NIST in particular should be closely monitored to assess requirements on the horizon. Add a footnote here: Moreover, the Federal Risk and Authorization Management Program (FedRAMP) and the Department of Defense Cybersecurity Maturity Model Certification (CMMC) are frequently incorporated into contracts under the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS), which may impose additional obligations.

DOJ's announcement may also trigger increased interest among the FCA relators' bar, which routinely represents whistleblowers in bringing FCA suits in the name of the government. The initiative may well spur company insiders to consider filing suit over perceived cybersecurity violations with an eye toward receiving the relators' share of any proceeds, which can total 30% of any recovery. For example, individuals who disagree with an organization's decision not to report a potential data breach or to delay reporting a breach pending an investigation to fully understand its scope may opt to file suit, alleging that the failure rendered the organization's grant-related assurances false.

Companies pursued under this initiative may of course have numerous defenses to FCA liability in those scenarios. For one, it is far from clear that violations of cybersecurity standards would be considered material to government payment decisions under the Supreme Court's decision in *Universal Health Services, Inc. v. Escobar*.[6] But this announcement presents an important opportunity for health care and life sciences companies to avoid the risk and distraction of DOJ scrutiny and *qui tam* litigation by taking steps now to address any vulnerabilities.

Key Takeaways

Health care and life science companies that may fall within the reach of this new initiative may consider conducting a review of their cybersecurity and risk management practices for consistency with NIST and other relevant frameworks.[7] For companies already subject to HIPAA, such a review may already be part of the entity's HIPAA security risk analysis; for entities not covered by HIPAA, implementing or augmenting a cybersecurity program to align with NIST standards may require significant resources and investment.

---

[4] The White House, FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity (Aug. 25, 2021), available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.

[5] Pursuant to the January 2021 amendment to Health Information Technology for Economic and Clinical Health (HITECH) Act, the Department of Health and Human Services must consider specific "recognized security practices" of covered entities and business associates under HIPAA when making certain determinations regarding fines, penalties, and other remedies related to HIPAA violations. "Recognized security practices" is defined by the Act to mean the standards, guidelines, best practices, methodologies, procedures, and processes developed under the NIST framework, in addition to other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities. See https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf.

[6] *Universal Health Services, Inc. v. United States ex rel. Escobar,* 136 S. Ct. 1989 (2016) (holding that "the implied false certification theory can be a basis for False Claims Act liability when a defendant submitting a claim makes specific representations about the goods or services provided, but fails to disclose noncompliance with material statutory, regulatory, or contractual requirements that make those representations misleading with respect to those goods or services.").

[7] For example, the amendment of the HITECH Act also directed HHS to review an organization's recognized security practices developed under section 405 of the Cybersecurity Act of 2015.

Given the initiative's emphasis on timely identifying and reporting breaches, health care and life science companies should prioritize a review of their incident response process, including:

- **Ensuring the entity has implemented a documented, robust incident security response plan.** As a best practice, the plan should be reviewed and updated at least annually through a formalized internal review process to ensure the plan addresses changes in criticality, business value, and changes in applicable legal requirements.

- **Documenting reporting trees and methods within the incident response plan.** Reporting trees should account for all possible scenarios and should include options to communicate incidents that are not reliant on the entity's IT infrastructure, which, depending on the incident, may be decommissioned.

- **Instituting tabletop exercises and drills in accordance with the incident response plan to ensure the entity is adequately prepared for an incident response.** Such exercises and drills should be appropriately scoped to each function and should include adequate training regarding responsibility to report incidents, to whom incidents should be reported, and, for management-level individuals, the proper handling of such reports.

- **Identifying and engaging external partners to assist in the event of an incident.** In order to efficiently respond to cybersecurity incidents, entities should identify external partners to assist in incident response, investigation, mitigation, and notification efforts, who either have already been retained, or who may be otherwise quickly engaged should an incident occur. Key partners may vary by the entities' specific cybersecurity profile and risks, but may include forensic/IT support, legal support, risk/insurance support, and public relations/consulting support.