# DOJ-HHS Announces False Claims Act Working Group, Emphasizes Healthcare Fraud Enforcement Priorities

 The Trump administration recently announced the renewal of a new cross-agency collaboration between the Department of Justice (DOJ) and the Department of Health and Human Services (HHS) in the form of the **DOJ-HHS False Claims Act Working Group**. The Working Group will be jointly led by Deputy Assistant Attorney General (DAAG) of the Commercial Litigation Branch Brenna Jenny, HHS Acting General Counsel Sean Keveney, and HHS Office of Inspector General Acting Chief Counsel Susan Edwards, and will include the Centers for Medicare & Medicaid Services (CMS) Center for Program Integrity and U.S. Attorneys' Offices.

Read the full alert **here.**

---

# Whistleblower Lawyers Use False Claims Act to Target Private Equity Firms Invested In Healthcare and Life Sciences

Recent developments demonstrate that the health care industry – including life sciences companies – continues to be subject to heightened regulatory scrutiny and enforcement risk. This alert addresses the U.S. Department of Justice ("DOJ") use of the False Claims Act ("FCA") to pursue private equity investors and their portfolio companies, including life sciences companies. While DOJ has been actively investigating private equity portfolio companies, the driver behind the majority of DOJ's investigations are whistleblower plaintiff lawyers who file *qui tam* suits alleging FCA violations. These lawyers have found a receptive audience in both legislative and executive branches of the federal government and are bringing pressure on DOJ to ramp up its focus on the private equity industry, a perceived deep-pocket in FCA cases. Our lawyers **Kirk Ogrosky**, **Anne Railton**, **John**

**LeClaire** and **Chris Wilson** examine the issue in this **client alert**.

---

# DOJ Announces New Initiative to Use False Claims Act to Enforce Compliance with Data Privacy and Security Laws and Contract Requirements

The Department of Justice recently announced the launch of its new Civil Cyber-Fraud Initiative (the "Initiative") which intends to use the False Claims Act to pursue "cybersecurity-related fraud by government contractors and grant recipients."

Specifically, the Initiative will target those who:

1. knowingly provide deficient cybersecurity products or services,
2. knowingly misrepresenting their cybersecurity practices or protocols, or
3. knowingly violate obligations to monitor and report cybersecurity incidents and breaches.

This new initiative significantly expands the potential liability of federal contractors and healthcare provider that participate in federal healthcare programs related to data privacy and cybersecurity issues.

*False Claims Act*

The False Claims Act broadly prohibits anyone from, among other things, knowingly presenting, or "causing to be presented" a false claim for payment if the claim will be paid directly or indirectly by the federal government. The False Claims Act is the government's main enforcement tool for fighting healthcare fraud, with over $2.2 billion recovered in 2020.  Penalties for False Claims Act violations include three times the actual damages sustained by the government, mandatory civil penalties of between $11,181 and $22,363 for each separate false claim, and attorneys' fees and costs. Further, the False Claims Act allows whistleblowers to bring lawsuits on behalf of the federal government. Also known as a "qui tam" realtor, a whistleblower who brings a successful *qui tam* action can receive 15 to 30 percent of the damages the government recovers from the defendants. The ability for an individual within one's own organization to raise flags with the federal government under the False Claims Act especially heightens risk.

*HIPAA*

Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), "covered entities" and their "business associates" are subject to certain obligations and limitation related to

their use and disclosure of "protected health information" ("PHI"). Covered entities are health care providers, health plans and health care clearing houses that transmit any information in an electronic form in connection with a transaction for which HHS has adopted standards. A business associate is a person or entity that performs certain services for or functions on behalf of the covered entity that involve the use or disclosure of PHI. Finally, PHI is any individually identifiable information, including demographic data, that relates to an individual's past, present or future health or payment for the provision of healthcare.

The obligations imposed on covered entities and business associates under HIPAA include maintaining and following specific privacy and security policies and procedures regarding access to, use, processing, transfer, storage, and disclosure of PHI and implementing physical, technical, and administrative safeguards to protect the privacy and security of PHI. In addition, covered entities are required to notify affected individuals, the Department of Health and Human Services, and, for certain larger breaches, the media of data breaches. Similarly, business associates are required to notify covered entities of data breaches.

*Implications*

The goal of holding accountable those who "knowingly provide deficient cybersecurity products or services, knowingly misrepresent their cybersecurity practices or protocols, or knowingly violate obligations to monitor and report cybersecurity incidents and breaches" presents particular risk for covered entities and their business associates.

For example, consider a revenue cycle management ("RCM") company that submits claims on behalf of a healthcare provider (including claims to government payors) that experiences a security incident, conducts a HIPAA risk assessment, and shares that assessment with the Covered Entity customer who determines the RCM company did not implement the necessary physical, technical and administrative safeguards required under HIPAA. Could the customer, the government, or a whistleblower allege that the RCM company knowingly misrepresented its cybersecurity practices or protocols and thereby caused the submission of false claims?

Further, consider an electronic health records company ("EHR") that is certified by the Office of the National Coordinator who experiences a breach of unsecured PHI, conducts a HIPAA risk assessment and determines it is not obligated to report the breach based on a low risk of compromise in accordance with 45 C.F.R. 164.402. Could the government or a whistleblower allege that the EHR company failed to report a breach and thus caused the submission of false claims by healthcare providers that use its EHR and are able to avoid reductions in Medicare reimbursement by using a certified EHR?

False Claims Act cases are commonly pursued under what is known as the "false certification theory". A claim is considered false when a claimant "certifies compliance with a statute or regulation as a condition to governmental payment." The false certification theory considers a claimant's *request* for payment as "implied certification" of compliance with said statutes or regulations. Despite the broad implications of the false certification theory, there is some check on the ability of the government or a whistleblower to bring cases on failure to comply with HIPAA through what is known as the materiality requirement under the False Claims Act. In *Universal Health Services v. United States ex rel. Escobar*, the U.S. Supreme Court held that the government and whistleblowers bear the burden of proving the "rigorous and demanding" materiality requirement under the False Claims Act. The Supreme Court further stated that the False Claims Act is "is not a means of imposing treble damages and other penalties for *insignificant* regulatory or contractual violations." Accordingly, the government and whistleblowers must demonstrate that allegedly insufficient technical safeguards or that an alleged failure to report a breach are actually

*material* to the government's payment decision.

The potential use of the False Claims Act to enforce HIPAA compliance may also change how due diligence is conducted on covered entities who bill government payors and their and business associates. While security incidents are common, the potential for liability under the False Claims Act related to such an incident increases the importance of conducting thorough diligence related to such incidents. The importance of conducting due diligence on a seller's compliance with HIPAA's requirements related to administrative, technical, and physical safeguards is also magnified by the potential for liability under the False Claims Act for failure to comply with those requirements. The risk related to conducting a risk assessment related to a data breach is similarly increased and such assessments should be scrutinized carefully in due diligence.

---

# Senate Judiciary Committee Advances False Claims Act Amendment to Full Senate

On October 28, a majority of members on the Senate Judiciary Committee voted 15-7 to advance to the full Senate a bipartisan bill that would make a number of amendments to the False Claims Act ("FCA"), including one that would make significant changes to the FCA's definition of "materiality." Senator Chuck Grassley of Iowa, who serves as the ranking member of the Judiciary Committee, argued for the materiality amendment, stating that it is intended to correct the "misinterpretations" of the FCA "created by the *Escobar* court."

Under the FCA, only a material violation – one that has "a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property by the government" – can form the basis for liability. The Supreme Court in *Universal Health Services v. United States ex rel. Escobar* stated that the FCA's materiality standard is "rigorous" and "demanding," and held that a violation of a particular requirement would likely not be considered material if (for example) the government had actual knowledge of the violation and chose to pay the claim anyway.

The materiality amendment advanced to the full Senate would undo the protections offered by the *Escobar* ruling, and instead states that "in determining materiality, the decision of the government to forego a refund or pay a claim despite actual knowledge of fraud or falsity shall not be considered dispositive if other reasons exist for the decision of the government with respect to such refund or payment."

The number of suits filed under the *qui tam* provisions of the FCA are steadily increasing over the years, with **672 *qui tam* actions filed in 2020** alone. Should this FCA amendment be enacted, its lowered materiality standard will make it significantly more difficult for defendants in *qui tam* actions to win motions to dismiss on materiality grounds, or to obtain summary judgment; as a

result, many more of these cases will move forward to more expensive and time-consuming stages of litigation.

Health care providers and other health care companies who are the potential defendants in FCA cases already often spend significant resources defending against these claims. While the proposed amendment advanced by the Judiciary Committee last week is intended to reduce fraud and abuse – for example, the amended materiality standard would be particularly important in situations in which the government is aware of fraudulent claims but is unable or unwilling to stop paying for the provision of critical healthcare services***; but, it may also have an effect on the overall costs of defending a claim, whether or not meritorious.  We will continue to monitor updates with respect to the FCA and related legislation.***

---

# PE Investment in Health Care Attracting Greater Federal Scrutiny


Private equity investment in health care companies has garnered increasingly critical attention from the federal government, including recent scrutiny by Congress in March 2021, when the Oversight Subcommittee of the U.S. House of Representatives' Ways and Means Committee held a hearing on "Examining Private Equity's Expanded Role in the U.S. Health Care System."

The tenor of the hearing is encapsulated in the opening remarks of the Oversight Subcommittee's Chairman, U.S. Representative Bill Pascrell Jr. (D-N.J.), who kicked off the discussion by cautioning that: "It's past time for a bright light to be shined on how private equity ownership and our health care system affects patient safety, cost, and jobs." Noting that 2020 saw $66 billion in private equity investment across the health care industry — a 21% increase from 2019 — Chairman Pascrell expressed concern that "private equity's main focus — profit — is often at odds with what is best for patient care."

Read the **full *New York Law Journal* article**.

---

# Goodwin Webinar – Healthcare Issues +

# Trends: The False Claims Act and Other Government Enforcement

Healthcare companies are facing unprecedented challenges as a result of the COVID-19 crisis. This includes heightened enforcement risks. A key area of risk is the federal False Claims Act (FCA), a powerful tool for the DOJ to seek substantial penalties including three times the amount of money a company received in federal funds.

Join members of Goodwin's Healthcare team as they discuss recent enforcement developments and ways to mitigate risk from a panel of Goodwin lawyers with experience helping healthcare companies, their executives and medical professionals navigate enforcement investigations.

To register for this event, please visit the registration page **here**.