INVESTIGATION HYDRAS: NAVIGATING COMPLEX ISSUES IN INTERNAL INVESTIGATIONS

BY MICHAEL J. REGIER, JONATHAN A. PORTER[1] & JOHN H. LAWRENCE

AHLA Fraud and Compliance Forum
September 30-October 1, 2021
Baltimore, Maryland

I. Introduction[2]

Internal investigations function as a manifestation of a healthy compliance program. They assist organizations in and outside of health care to effectively assess and respond to internal and external risks, including those that may indicate organizational wrongdoing. Within health care, internal investigations can assist health care providers and institutions effectively respond to a myriad of issues, ranging from the potential receipt of overpayments, alleged kickback arrangements, and other equally varied issues raised by whistleblowers and/or government agencies.

This paper considers certain complex issues applicable to conducting health care fraud investigations. Specifically, this paper discusses considerations for investigative teams related to: (1) the scope of the investigation; (2) the use of experts; (3) quantifying an overpayment; and (4) disclosures. Each investigation has its own nuances and complexities and, as such, this paper is not intended to serve as a comprehensive review of all of the various considerations for counsel conducting internal investigations. The authors' goal is to provide both internal and external counsel a general framework for conducting efficient health care fraud investigations, from the initial scoping phase to the decision whether or not to disclose the findings of the investigation to enforcement agencies.

II. Scope of the Investigation

Internal investigations in health care are not "one-size fits all" and they must be tailored to the issues under investigation and the context in which the investigation occurs. One of the most frequent challenges with internal investigations is ensuring that they are appropriately scoped, especially within health care where an investigation can involve complex regulatory issues. Specifically, at the outset of an investigation, it is critical to establish the proper scope to ensure that the investigation is appropriately comprehensive without becoming too expansive. As part of this process, companies and external counsel should look to guidance from the Department of Justice ("DOJ") and the Office of Inspector General for the Department of Health and Human Services ("OIG"). Additionally, a properly scoped investigation requires an understanding of the client's corporate structure and the key issues at play in the investigation. Failing to do so may lead to inefficient investigations which are overly broad, unfocused, or too narrow in scope. As discussed further below, improperly scoped investigations may lead to increased costs to the client and unreliable factual findings. With this information in mind, the investigative team can

[1] The views expressed in this paper are the authors' own, and do not necessarily reflect the views of the United States Department of Justice.

[2] The authors would like to extend a special thanks to both Maggie Power and Megan Moore, associates at K&L Gates LLP, for their tremendous assistance in drafting this article.

thoughtfully establish a framework for conducting an efficient, thorough, and effective investigation.

A. Legal Standards

1. *Scope of Investigation*

Generally, companies and external counsel should consider guidance issued by the DOJ and OIG when scoping an internal investigation. In evaluating a corporate compliance program when deciding whether civil or criminal liability exists or during its negotiations with the subjects or targets of an investigation, the DOJ considers, *inter alia*, whether the company has engaged in *properly scoped* investigations conducted by qualified personnel as part of its compliance program.[3] As part of this analysis, the DOJ will consider whether the company adequately triages complaints for further investigation and takes steps to ensure that these investigations are properly scoped based on the nature of the complaint.[4]

2. *Disclosure Obligations*

In order to gain cooperation credit for its internal investigation, DOJ guidance requires that the company "must disclose the relevant factors of which it has knowledge," including the identity of all individuals who were substantially involved in the misconduct.[5] Similarly, as part of the OIG's Self-Disclosure Protocol, the company must submit an investigative report which describes the nature and extent of the misconduct and the company's response to the matter.[6] The report must specifically include the identities of corporate officials who should have been aware of the misconduct, the impact of the misconduct on patient care, and potential causes for the misconduct.[7] In short, internal investigations and whether they are properly scoped play an important role in disclosures to the Government.

B. Understanding the Client and Sources of Relevant Information

When determining the scope of an investigation, it is critical to understand the client, its structure, and where to obtain relevant information. Key issues to understand, either through scoping interviews or other means, include:

- **Identity of the client.** Both internal and external counsel must carefully determine the identity of the client before beginning an investigation. For instance, depending on the nature of the investigation, the client could be the company itself or certain company executives or employees.
- **Relevant corporate structure and information flow.** The investigative team must understand the flow of information within the relevant business units. Developing this

---

[3] U.S. DEP'T OF JUST., CRIM. DIV., EVALUATION OF CORPORATE COMPLIANCE PROGRAMS 7 (June 2020), https://www.justice.gov/criminal-fraud/page/file/937501/download/.

[4] *Id.*

[5] U.S. Dep't of Just., Justice Manual § 9-28.720 (2017), https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.720.

[6] Publication of the OIG's Provider Self-Disclosure Protocol, 63 Fed. Reg. 58,399, 58,401 (Oct. 30, 1998).

[7] *Id.*

understanding could be accomplished by a review of an organizational chart and/or through scoping interviews with relevant personnel.

- **Relevant decision makers and custodians.** At the outset, the investigation should aim to identify the relevant decision makers and custodians who would have access to potentially relevant materials. Decision makers include individuals who approved or are otherwise responsible for the decisions or policies at issue in the investigation. Custodians, on the other hand, may be a broader category including lower level employees with access to relevant documentation. The investigators may identify these individuals through document review and/or scoping interviews.
- **Storage of and access to relevant information.** Once the investigative team identifies the list of custodians, it must determine where the custodian stores relevant information and how the investigative team can access this information. For instance, the investigative team may conduct a document collection interview with each custodian, asking specific questions regarding the individual's use and storage of relevant documentation. Depending on the nature of the investigation, these interviews may be conducted in conjunction with an e-discovery or forensic document collection expert.

At each stage of this process, the investigative team should consider how to maintain applicable privileges and protections.

C. Understanding the Issues and Objectives

Additionally, the investigative team must thoroughly understand the issues at play in the investigation and the ultimate objective of the client. Key considerations include:

- **Investigation triggering events.** The investigative team must understand the origins of the investigation, including whether there was a whistleblower report, a request from a government entity, or an issue identified during a routine auditing process.
- **Issues to be resolved.** The investigative team should have a clear understanding of the issues to be considered during the investigation. This understanding may be bolstered by preliminary document review and/or through scoping interviews.
- **Client's investigation goals.** In order to properly scope the investigation, the investigative team must understand what issues the client wants to resolve and how the client hopes to resolve these issues. For instance, a client may wish to expand the scope of an investigation based on other business concerns, or may want to constrain the scope of an investigation based on its understanding of its business structure. The investigative team should keep these goals in mind while formulating the investigative scope.
- **Efficiency.** Efficiency is critical to a properly scoped investigation. As discussed further in Section I.D below, overbroad and inefficient investigations often do more harm than good. The investigative team should consider how to efficiently achieve the client's goals, given the nature of the issues and government guidance regarding internal investigations.
- **End game.** At every step of the scoping process, the investigative team should consider the possible courses of action if the investigation finds that misconduct likely occurred. For instance, internal investigations may lead to self-disclosures to the government or internal corrective actions (e.g., compliance policy updates or termination of employees involved in misconduct).

D. Common Internal Investigation Scoping Problems

1. *Scorched Earth*

Investigative teams sometimes conduct "scorched earth" investigations, which are overly broad given the issues, consequences, and nature of the client's business. For instance, the investigation team may attempt to interview every potentially relevant employee and review every document that *might* be at issue. A "scorched earth" investigation risks uncovering issues which are not relevant to the matter, as well as increasing the client's investigative costs.

2. *Scattershot*

Additionally, internal investigations may be too "scattershot" or unfocused if the investigation is unorganized and not tied to a clear investigative work plan. A "scattershot" investigation risks overlooking key issues and may also increase the costs of the investigation.

3. *The Trees for the Forest*

Investigations may also be scoped too narrowly, leading to an investigation which does not comprehensively address all the relevant issues. In fact, an investigation which is too narrowly scoped may result in inadequately addressing the primary concerns at issue. Additionally, investigations which are too narrow may produce unreliable results and, paradoxically, increase the ultimate cost of the investigation, if supplemental investigative phases are necessary.

E. Structuring an Effective and Credible Investigation

To structure an effective and credible investigation, the team must clearly define the scope and protocol of the investigation at the outset. This may include developing "tranches" of review and investigation based on priority and the team's preliminary understanding of the issues. Additionally, the investigative team should establish apparent and centralized internal reporting channels to ensure clear communication within the team and to the client. Throughout the entire investigation, the team should actively consider measures to maintain attorney-client privilege and attorney work product protection. The team should carefully consider distribution of privileged and protected materials to those outside of the team. As the investigation progresses, the team should also begin to coordinate information necessary for remediation and/or disclosure to a government entity.

III. Use of Experts

Internal and external experts can be essential members of an investigative team; however, there is some risk that these experts may become a *qui tam* relator in the future. As such, the investigative team must carefully consider when and how to engage an expert, as well as how to maintain privilege over information communicated to the expert.

A. When to Engage a Consultant or Other Expert

When considering whether to engage a consultant or expert during an investigation, the team may consider the following factors:

- **Subject matter expertise.** During investigations, it is often necessary to engage a consultant due to the complex and specialized nature of the issues. For instance, in billing

cases, consultants can analyze complex datasets and provide conclusions regarding the company's billing practices to the investigative team.

- **Surge capacity and time constraints.** At times, it may be necessary for an investigative team to engage a consultant to increase the team's capacity, especially when faced with urgent time constraints. For instance, if an investigation coincides with a relevant contractual renewal period, it may be necessary to accelerate the review process with the assistance of a consultant or expert in order to make a timely recommendation to the client. In addition, where the provider believes a compliance concern may have resulted in overpayments by Federal programs, use of external resources may also be necessary to assist the provider in meeting the timeline for returning identified overpayments under Federal law.[8]
- **Objectivity.** The evaluation of an external expert often carries more weight due to perceived objectivity than the analysis of an internal investigation team. For instance, the conclusions of a respected external expert regarding the propriety of the company's actions may carry more weight with the government than internal conclusions.
- **Relationships with key enforcement authorities.** Finally, the investigation team may decide to engage an expert due to the expert's relationship with key enforcement authorities. For instance, engaging an expert that formerly worked for the DOJ or OIG may increase the government's reliance on the expert's opinion and analysis.

B. Privilege Considerations

Generally, consultants are engaged through counsel, either internal or external, to support privilege over material provided to and/or produced by the consultant. These experts frequently engage on sensitive subject matters with potentially serious consequences with the company. Additionally, the client often only has limited insight into the full scope of the issue at the outset of the investigation, making maintaining privilege even more critical. Counsel and client may more freely determine whether, when, and how to act upon the findings and recommendations of the consultant if privilege is maintained. The investigative team should consider the two key privileges: attorney-client privilege and attorney work product doctrine. As discussed below, each privilege has slightly different scope and impact.

1. *Attorney-Client Privilege*

Attorney-client privilege is an evidentiary rule making communications between attorney and client confidential. The privilege promotes full, frank, and open conversations between client and counsel. In order for attorney-client privilege to apply, the following requirements must be met:[9]

- Communication must be for the purpose of obtaining legal advice or assistance in a legal proceeding;
- Communication must have been made in confidence;
- Communication must have been made by the client, and not a third party;
- Recipient of communication must be an attorney who was acting as an attorney at the time the communication was received; and

[8] *See* 42 C.F.R. § 401.305(b)(1); *see also* Section IV.A, *infra.*

[9] *See, e.g.*, *Colton v. U.S.*, 306 F.2d 633, 637 (2d Cir. 1962).

- Party asserting the privilege must be a client.

2. *Attorney Work Product Doctrine*

On the other hand, the attorney work product doctrine provides *qualified immunity* from discovery of certain materials prepared in anticipation of litigation.[10] The protection allows attorneys to explore and develop alternate lines of inquiry or theories of the case without concern that they could later be discovered in litigation. Because the immunity is qualified, a showing of undue hardship or injustice may still allow the opposing party to obtain discovery of the work product materials.[11] Specifically, the doctrine covers the attorney's written statements, private memoranda, and personal observations *made in anticipation of litigation*. A potential regulatory violation and/or compliance reporting obligation may not always be sufficient to support the conclusion that litigation is anticipated.

The protection generally extends to cover materials prepared by a third-party agent other than an attorney, such as a consultant engaged by the attorney.[12] If the report or statement by the consultant was made without an attorney's direction or supervision, they may be deemed discoverable "ordinary course of business" communications. Thus, it is important for the investigation team to carefully manage directions provided to the consultant, as discussed in Section II.C below.

C. Structuring Engagement with Consultant

To best protect the interests of the company and the integrity of the investigation, the team should consider the following when structuring its engagement with a consultant:

- **Retain through counsel (external or internal).** As discussed above, this is critical for the maintenance of the attorney work product doctrine protections.
- **Purpose of the engagement.** Clearly define the purpose of the engagement and its relationship to anticipated litigation.
- **Scope of the engagement.** The scope of the engagement should be limited based on the scope of the larger investigation and should be tied to the anticipated litigation.
- **Intention that engagement and work product are privileged.** The engagement letter should affirmatively state that the engagement and associated work product are covered by the attorney-client privilege and attorney work product doctrine.
- **Communications from the consultant.** The investigation team should ensure that communications to/from the consultant are funneled through an attorney control group to ensure that all work product generated by the consultant is at the direction of an attorney.
- **Supervision and monitoring of consultant's work.** The investigation team should carefully supervise and monitor the consultant's work to prevent designation of the work product as an "ordinary course of business" communication. For instance, the investigation team should review and comment on the consultant's work product.

---

[10] *See, e.g.*, *Hickman v. Taylor*, 329 U.S. 495 (1947) (establishing attorney work product doctrine); Fed. R. Civ. Pro. 26(b)(3).

[11] Fed. R. Civ. P. 26(b)(3).

[12] Fed. R. Civ. P. 26(b)(3).

- **Interplay with litigation hold.** As discussed above, the attorney work product privilege applies only to documents generated *in anticipation of litigation.* As such, the litigation hold issued by the company may be useful guidance for the investigation team when determining the purpose and scope of the consultant's engagement.

D. Is Your Consultant Your Next Relator?

Retained consultants often have detailed access to information about the client's systems, processes, and compliance concerns. Because of this, consultants frequently have access to information which may serve as the basis for a future *qui tam* complaint. Becoming a relator may be attractive to the consultant or members of the consultant's team due to the potential whistleblower rewards. To mitigate this risk, the investigation team should consider adding specific contractual provisions designed to limit the consultant's ability to effectively serve as a relator.

1. *Representations and Warranties*

The engagement may include a requirement for confidentiality and non-disclosure agreements for the consultant's team. Additionally, the investigation team may require the consultant and its team to sign an acknowledgement regarding the client's compliance program and its application to the consulting team. The acknowledgement may further require the consultant to report issues to the client's compliance team before reporting to any third party. Finally, the investigation team may require the consultant to represent that no one on the consulting team has acted as a *qui tam* relator with respect to the client, or any current or former client.

2. *Covenants*

The investigation team may require that the consultant agree to various covenants to prevent disclosure to a third party. For instance, the consultant may be required to disclose to the client any non-compliance identified, whether or not within the scope of the engagement. The consultant may further be required to work in good faith with the client to identify and resolve these identified instances of non-compliance. A covenant may also include a provision requiring escalation within the client of non-compliance or perceived failures to remediate before disclosing the concerns to a third party. If the consultant does intend to disclose compliance concerns, a covenant may also impose a requirement that disclosure to a third party cannot be made without: (a) written notification to the Chair of the client's Board of Directors (or Board Committee established to deal with compliance matters) and (b) reasonable period of time for Board (or Board Committee) to review, respond and remediate.

3. *Termination and Remedies*

The agreement may provide for certain remedies in case of a breach of these covenants. For instance, the agreement may state that a breach will result in an immediate termination, fee forfeiture and/or fee clawback, and liquidated damages.

IV. Quantifying an Overpayment

Conducting an effective and properly scoped internal investigation in health care can often involves determining whether an overpayment has occurred and, if so, how to effectively quantify it. Set forth below are the legal standards framing how investigative teams and their providers must navigate potential overpayments, as well as related key considerations. Quantifying overpayments

that are identified during the course of an investigation can present some of the most challenging aspects of the investigation itself due to the complexity of overarching regulatory issues; the volume and diversity of data at issue; and the availability of information.

A. Legal Standard

1. *The Patient Protection and Affordable Care Act of 2010*

Section 6402(a) of the Patient Protection and Affordable Care Act ("ACA") established a new section 1128J(d) of the Social Security Act, codified at 42 U.S.C. § 1320a-7k(d), which "requires a person who has received an overpayment to report and return the overpayment to the Secretary, the state, an intermediary, a carrier, or a contractor, as appropriate, at the correct address, and to notify the Secretary, state, intermediary, carrier or contractor to whom the overpayment was returned in writing of the reason for the overpayment." Such overpayment must be reported and returned by either "(i) sixty (60) days after the date on which the overpayment was identified, or (2) the date any corresponding cost report is due," whichever is later.[13] This overpayment rule applies to a provider of services, supplier, Medicaid managed care organization, Medicare Advantage organization, and prescription drug plan sponsors (collectively referred to herein as "providers").[14]

2. *Overpayment Rule*

A proposed rule implementing this overpayment provision was issued on February 16, 2012.[15] Exactly four years later, on February 16, 2016, the Centers for Medicare and Medicaid Services ("CMS") issued its final rule entitled "Medicare Program; Reporting and Returning of Overpayments." ("Overpayment Rule").[16] The Overpayment Rule established regulations at 42 C.F.R. subpart D and further amended other regulations to set forth the process for reporting and returning overpayments.

Echoing the above statute, the Overpayment Rule brought about 42 C.F.R. § 401.305(b)(1), which also states that "[a] person who has received an overpayment must report and return the overpayment by the later of either of the following: (i) [t]he date which is 60 days after the date on which the overpayment was identified; [or] (ii) [t]he date any corresponding cost report is due, if applicable."

The statute and regulations define an "overpayment" as "any funds that a person has received or retained under title XVIII of the [Social Security] Act to which the person, after applicable reconciliation, is not entitled under such title."[17] This standard is applied regardless of fault; the provider did not have to intend to bill Medicare incorrectly for an overpayment to occur.

---

[13] 42 U.S.C. § 1320a-7k(d)(2)(A)-(B).

[14] *See* 42 U.S.C. § 1320a-7k(d)(4)(C)(i).

[15] *See* Medicare Program; Reporting and Returning of Overpayments, 77 Fed. Reg. 9179.

[16] 81 Fed. Reg. 7654.

[17] 42 U.S.C. § 1320a-7k(d)(4)(B); 42 C.F.R. § 401.303.

Additionally, overpayments can include payments received for non-covered services, errors on a Medicare cost report, and coding errors, among others.

i. Identifying Overpayments

As noted above, the time period for returning an overpayment is generally within sixty (60) days of when it has been "identified."[18] The regulations provide that an overpayment is identified when a person "has, or should have through the exercise of reasonable diligence, determined that the person has received an overpayment and quantified the amount of the overpayment."[19] As stated, it is expected that providers will use "reasonable diligence" in identifying overpayments.[20] The Overpayment Rule describes reasonable diligence as "both proactive compliance activities conducted in good faith by qualified individuals to monitor for the receipt of overpayments and investigations conducted in good faith and in a timely manner by qualified individuals in response to obtaining credible information of a potential overpayment."[21] Described in the Overpayment Rule as the "ostrich defense," CMS makes clear that under this standard, it is the "plain mandate to report and return overpayments received, [and this cannot] avoided by not taking action to obtain actual knowledge of an overpayment."[22]

The number of years a provider must review data to determine if an overpayment has occurred—known as the "lookback period"—is "within 6 years of the date the overpayment was received."[23]

ii. Time Permitted to Identify an Overpayment

Once a provider receives "credible information" that an overpayment exists a provider must conduct a "timely investigation," which the Overpayment Rule states is "at most 6 months from receipt of the credible information, except in extraordinary circumstances.[24]" Thus, "[a] total of 8 months (6 months for timely investigation and 2 months for reporting and returning)" is allotted for identifying and reporting an overpayment.[25]

Regarding what constitutes "credible information," CMS stated that this standard means "information that supports a reasonable belief that an overpayment may have been received."[26] Importantly, it also stated that "[d]etermining whether information is sufficiently credible to merit an investigation is a fact-specific determination."[27]

---

[18] *See* 42 U.S.C. § 1320a-7k(d)(2)(A); 42 C.F.R. § 401.305(b)(1)(i).

[19] 42 C.F.R. § 401.305(a)(2).

[20] *Id.*

[21] 81 Fed. Reg., at 7661.

[22] *Id.* at 7660

[23] 42 C.F.R. § 401.305(a)(2).

[24] *Id.* at 7662.

[25] *Id.*

[26] *Id.*

[27] *Id.* at 7663.

iii. Reporting and Returning the Overpayment

The above discussed deadlines are suspended if or when the provider files a submission through either the OIG Self-Disclosure Protocol or the CMS Voluntary Self-Referral Disclosure Protocol.[28] If either disclosure option is utilized, then the deadline for returning an overpayment will continue to be suspended until a settlement agreement is entered, or the provider withdraws or is removed from the applicable provider disclosure protocol.[29]

If the provider does not choose to file a submission through either the OIG or CMS protocols, then a "person must use an applicable claims adjustment, credit balance, self-reported refund, or other reporting process set forth by the applicable Medicare contractor to report an overpayment."[30]

A more detailed discussion of reporting overpayments can be found at Section V, herein.

iv. Retaining Overpayments

If a provider retains an overpayment "after the deadline for reporting and returning the overpayment," it becomes "an obligation for purposes of 31 U.S.C. 3729."[31] Thus, the unlawful retention of the overpayment can expose a provider to liability under the federal False Claims Act, which may include treble damages and significant monetary penalties.[32]

B. Key Considerations

Providers must determine the scope of the potential overpayment, including the number of arrangements and/or claims made during the lookback period. Importantly, providers must also determine with the accessibility of information, such as claims data, within their organization. Overpayment investigations are time pressured, given the statutory requirement to report within sixty days of identification and the six-month limitation from the receipt of credible information. Other external pressures may include any imminent external governmental investigations or potential whistleblower actions.

As the scope and facts of the investigation begin to take shape, providers may find it helpful or even necessary to engage a consultant or expert to help refine the scope or provide input on identifying claims data. An expert may also help providers arrive at a final overpayment number, through accounting or extrapolation, if warranted. Additionally, consultants or the engagement of legal counsel can help providers decide their reporting options.

---

[28] *See* 42 C.F.R. § 401.305(b)(2)(i)-(ii).

[29] *Id.*

[30] 42 C.F.R. § 401.305(d)(1).

[31] 42 C.F.R. § 401.305(e).

[32] *See* 31 U.S.C. § 3729(a)(1)(G); *see also* 31 U.S.C. § 3729(b)(3) ("the term "obligation" means an established duty, whether or not fixed, arising from . . . the retention of any overpayment").

V. **Disclosures**

A. Consequences of Disclosure

Deciding not to return an overpayment may result in criminal or civil penalties, as well as other reputational or organizational consequences.

1. *Criminal*

i. 42 U.S.C. § 1320a–7b(a)(3)

Under 42 U.S.C. § 1320a–7b(a)(3), entitled "Criminal penalties for acts involving Federal health care programs," it is a criminal offense to "hav[e] knowledge of the occurrence of any event affecting (A) his initial or continued right to any such benefit or payment, or (B) the initial or continued right to any such benefit or payment of any other individual in whose behalf he has applied for or is receiving such benefit or payment, conceal[] or fail[] to disclose such event with an intent fraudulently to secure such benefit or payment either in a greater amount or quantity than is due or when no such benefit or payment is authorized." As noted, this standard requires "knowledge of an event affecting" a right to payment, such as an overpayment. Notably, this provision requires only disclosure of such event, but does not require repayment.

Those violating this section are guilty of a felony and if convicted, may be subject to a fine "of not more than $100,000 or imprisoned for not more than 10 years or both."[33] Those convicted may also be excluded from participating in federal healthcare programs, such as Medicare, for up to one year.[34]

While charges under this statutory provision are rare, the government still retains the ability to prosecute pursuant to this statute.[35]

ii. 18 U.S.C. § 1957

Pursuant to 18 U.S.C. § 1957, it a criminal offense to "knowingly engage[] or attempt[] to engage in a monetary transaction in criminally derived property that is of a value greater than $10,000 and is derived from specified unlawful activity." Here, failure to disclose an overpayment in violation of 42 U.S.C. § 1320a–7b(a)(3) is "specified unlawful activity" for purposes of this provision. Therefore, the movement of money after having knowledge of an overpayment may trigger liability under § 1957. Notably, a person may be charged with a violation of this statute even if they had no role in the initial claim that triggered overpayment liability, so long as the person had knowledge that the funds are criminally derived.

iii. 18 U.S.C. §§ 287, 1035, & 1347

The government may also pursue charges under 18 U.S.C. § 287, entitled "False, fictitious or fraudulent claims;" 18 U.S.C. §1035, entitled "False statements relating to health care matters;" and 18 U.S.C. §1347, entitled "Health care fraud." Importantly, though, each of these requires the

---

[33] 42 U.S.C. § 1320a–7b(a).

[34] *Id.*

[35] *See e.g., United States v. Anderson,* 605 F.3d 404 (6th Cir. 2010) (affirming conviction under § 1320a–7b(a)(3) and affirming imposition of a 24-month sentence).

government to prove knowledge at the time of the claim, statement, or fraudulent activity. Yet, proof of later knowledge may be used as evidence to imply knowledge at the time of the claim, statement, or fraudulent activity in question.

iv. 18 U.S.C. § 4

The government may also charge a defendant under 18 U.S.C. § 4, entitled "Misprision of felony." This provision states that "[w]hoever, having knowledge of the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined under this title or imprisoned not more than three years, or both." Thus, knowledge of an "actual commission of a felony" must be shown.

2. <u>*Civil*</u>

Claims brought pursuant to the federal False Claims Act ("FCA"), codified at 31 U.S.C. § 3729, are perhaps the most well-known consequence of failing to report an overpayment. Specifically, the FCA prohibits, among other things, "knowingly present[ing], or cause[ing] to be presented, a false or fraudulent claim for payment or approval."[36] The FCA also prohibits "knowingly mak[ing], us[ing], or caus[ing] to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government."[37] This latter prohibition is commonly known as the "reverse" false claims theory.

Notably, violations of the FCA may result in statutory penalties for each discrete false claim, as well as "3 times the amount of damages which the Government sustains because of the act of that person."[38] However, a provider may potentially reduce their financial penalty if "the person committing the violation of this subsection furnished officials of the United States responsible for investigating false claims violations with all information known to such person about the violation within 30 days after the date on which the defendant first obtained the information."[39] If this occurs, then "the court may assess not less than 2 times the amount of damages which the Government sustains because of the act of that person."[40]

The FCA's *qui tam* provisions also create a major financial incentive for whistleblowers, known as "relators," to attempt to disclose conduct prior to the provider doing so. Pursuant to 31 U.S.C. § 3730(b)(1), "[a] person may bring a civil action for a violation of section 3729 for the person and for the United States Government." If the claim is successful, the relator may ultimately "receive at least 15 percent but not more than 25 percent of the proceeds of the action or settlement of the claim."[41] Additionally, the government retains the ability to intervene in claims that are

---

[36] *Id*. at 3729(a)(1)(A).

[37] *Id.* at 3729(a)(1)(G)

[38] *Id.* at 3729(a)(1) (the "FCA multiplier").

[39] *Id*. at 3729(a)(2)(A).

[40] *Id.* at 3729(a)(2).

[41] 31 U.S.C. § 37309(d)(1).

initially brought by a relator.[42] Therefore, if a provider discovers that it has presented a claim or claims that resulted in an overpayment, failing to timely return the overpayment to the Government can result in significant damages under the FCA, and there are tremendous incentives for insiders to become whistleblowers to report such reverse false claims.

3. *Other Consequences*

i. Corporate Integrity Agreements

The HHS OIG often "negotiates corporate integrity agreements (CIA) with health care providers and other entities as part of the settlement of Federal health care program investigations arising under a variety of civil false claims statutes."[43] These agreements are, at times, a significant undertaking for providers to ensure compliance, and can last for years. However, OIG may be less inclined to advocate for the imposition of a CIA if the provider is seen as proactively fixing the problem that gave rise to the case.

ii. Investigations

Another potential benefit of effectively self-disclosing an overpayment is that it may dissuade the government from launching a formal investigation into the matter, or if an investigation is still initiated, may limit its scope such that it is narrowly targeted to the disclosed issue. Conversely, failing to disclose may make the government more apt to conduct a thorough, wide-ranging investigation of the provider, thus potentially giving it the opportunity to uncover other conduct. However, disclosing does not prevent the government from instituting a thorough investigation of the provider. Moreover, those that choose to cooperate with the government must actually do so; cooperation credit is generally not given for those who do not fully cooperate. Lastly, self-disclosure and any subsequent investigations may orient the government and relators to be looking for similar conduct.

iii. Public Image

Additionally, from a public relations and image perspective, taking a proactive approach and self-disclosing conduct generally creates a better narrative, both in the provider's community and as to its board. Yet, self-disclosure does not necessarily insulate the provider from negative publicity.

iv. Derivative Actions

Those providers that are publicly traded could be subject to derivative actions or shareholder suits due to its disclosure.[44]

---

[42] *See d.* at 3730(b)(2) ("The Government may elect to intervene and proceed with the action within 60 days after it receives both the complaint and the material evidence and information.").

[43] *Corporate Integrity Agreements*, OIG https://oig.hhs.gov/compliance/corporate-integrity-agreements/index.asp (last visited August 30, 2021).

[44] *See In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).

v. Resource Intensive

Self-disclosure and the related investigation are both time- and resource-intensive activities. Frequently, these require the hiring of outside counsel, experts, and consultants, and may require employees of an organization to divert their attention to such investigation in addition to conducting their usual job duties.

B. Scope and Procedure of Disclosure

1. *Overpayment Only*

If an investigation determines that the disclosure is limited to an overpayment, then disclosure to the applicable Medicare Administrative Contractor ("MAC") is likely appropriate. This may include items such as overpayments resulting from incorrect coding or other coding errors, insufficient documentation, certain medical necessity errors, and other processing and administrative errors.

As noted herein, such overpayment must be disclosed within sixty days of the identification of the overpayment. Next, the MAC generally issues a demand letter detailing the amount of the overpayment and reasoning behind its calculation. This letter also typically sets forth the process for rebutting this overpayment demand, such as asking the MAC to consider new evidence or the provider providing an explanation and why it should offsets some or all the liability. Additionally, if the provider still disagrees with a MAC's determination, it may initiate an appeal.[45]

Providers are also given repayment options including an immediate payment; an immediate recoupment, which is offset against future payments; a standard recoupment, which is offset according to a schedule; and an extended repayment schedule, if the provider is unable to repay the overpayment within a required timeframe.

2. *More than Overpayment*

If the to-be-disclosed activity is more than an overpayment, or is a certain type of overpayment, then use of the OIG or CMS self-disclosure protocols is likely appropriate. For example, if the overpayment is not an isolated incident, or if the disclosed activity involves upcoding, billing for an excluded provider, duplicate billing, systemic or long-term errors, altered or falsified records, kickbacks, or other types of potential fraud, then disclosure through the OIG Self-Disclosure Protocol is likely appropriate.

To disclose such conduct, the provider submits a written disclosure to the OIG.[46] Then, the OIG investigates, verifies, and audits the disclosure.

A similar process is used for those disclosing a violation of 42 U.S.C. § 1395nn, known as the physician self-referral or "Stark" law. These disclosures are submitted to CMS via its

---

[45] *See, e.g., Original Medicare (Fee-for-service) Appeals*, CMS (July 20, 2021) https://www.cms.gov/Medicare/Appeals-and-Grievances/OrgMedFFSAppeals.

[46] *See Provider Self-Disclosure Protocol,* OIG https://oig.hhs.gov/compliance/self-disclosure-info/protocol.asp (last visited August 30, 2021).

Voluntary Self-Referral Disclosure Protocol.[47] Additionally, overpayments resulting from government contracts and grants have their own disclosure protocols.[48]

In some instances, providers may be able to disclose directly to the Department of Justice. Some United States Attorney's offices provide greater flexibility in settlement negotiations including identifying and applying the FCA multiplier, permitting payment over time, and taking into account a provider's ability to pay.

Overall, disclosure generally permits the provider to have better control over the scope of an investigation and obtaining an FCA release forecloses the opportunity for relators to file *qui tam* actions.

3. *Timing of Disclosure*

If a provider chooses to disclose prior to a government investigation being initiated, then they are likely entitled to a reduced FCA multiplier. However, claims brought by relators are not foreclosed until an FCA release is granted or there is public disclosure of the disclosed activity. As noted above, choosing to disclose prior to an investigation being initiated may give the provider more control over the ultimate scope of the investigation.

However, if a provider chooses to disclose during the pendency of an investigation, there is a possibility that they will still be given a more favorable FCA multiplier. Yet, there is still significant risk of failing to disclose until an investigation, especially for those cases that potentially have company-wide financial implications.

VI. Conclusion

As discussed herein, when conducting internal investigations, providers are frequently required to juggle competing concerns and risks during both the investigation and disclosure processes. Such concerns and risks are not only internally imposed by the organization and its stakeholders, but also by potential civil liability—emanating from both the government and private actors—as well as potential criminal implications. Thus, intentionally structuring the internal investigation to mitigate these risk, as much as possible, may help to prevent unexpected or unaccounted for consequences as the investigation unfolds. Additionally, engaging the correct consultants, experts, and legal counsel, and understanding the risks that such engagement may entail, may help providers successfully navigate these inevitably stressful and high stakes situations.

---

[47] *See Self-Referral Disclosure Protocol*, CMS (Oct. 22, 2019) https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/Self_Referral_Disclosure_Protocol.

[48] *See Contractor Self-Disclosure Program*, OIG https://oig.hhs.gov/compliance/self-disclosure-info/contractor.asp (last visited August 30, 2021); *HHS OIG Grant Self Disclosure Program*, OIG https://oig.hhs.gov/compliance/self-disclosure-info/grant.asp (last visited August 30, 2021).