Washington Health Law Manual – Fourth Edition
Washington State Society of Health Care Attorneys (WSSHA)

Chapter 10: Government Investigations of Health Care Providers

Author: Michael D. McKay (Seattle)
Organization: K&L Gates LLP

Author: Clifford C. Histed (Chicago)
Organization: K&L Gates LLP

Author: John C. Rothermich (Portland)
Organization: K&L Gates LLP

Author: Aaron E. Milstein (Seattle)
Organization: K&L Gates LLP

For reference purposes, this chapter was prepared from laws, cases, and materials selected by the authors, which were available as of September 28, 2021.

Biographies

Michael D. McKay, Author
Mike McKay is a partner in the Seattle office of K&L Gates LLP. As a former U.S. Attorney for the Western District of Washington, Mike's practice focuses on white collar criminal defense, internal investigations, and complex civil litigation, including government enforcement actions and civil cases with parallel criminal proceedings. Mike has worked on numerous cases involving investigations of health care providers and medical professionals, as well as related litigation. He has experience investigating and litigating issues arising under statutes such as the False Claims Act; Anti-Kickback Statute; various fraud, controlled substance, and pharmaceutical statutes; and analogous state-level laws. Mike assists clients in crafting and implementing comprehensive and tailored compliance programs and developing a corporate compliance structure to cultivate an environment of ethics, integrity, and efficiency. Mike has been asked by numerous private companies and municipal corporations to conduct investigations aimed at detecting and remedying fraud, waste, and other misconduct.

Clifford C. Histed, Author
Cliff Histed is a partner in the Chicago office of K&L Gates LLP and a former supervisory federal criminal prosecutor, supervisory government enforcement lawyer, state criminal prosecutor, and special agent with a federal inspector general's office. He has more than 30 years' experience investigating, prosecuting, and defending frauds and criminal offenses in highly regulated industries, including the securities and derivatives markets and health care. As a supervisory prosecutor, Cliff has approved search warrants, indictments, and plea agreements in many criminal health care cases. A seasoned trial attorney, Cliff has tried 27 cases in federal and state courts. He has supervised numerous federal criminal investigations and prosecutions, conducted internal investigations at companies in the health care industry and other highly regulated industries, and represented individuals served with government subpoenas. Cliff regularly speaks and writes on topics, including government investigations, enforcement actions, trends in criminal health care investigations, corporate compliance programs, and the prosecution of corporate entities.

John C. Rothermich, Author
John Rothermich is a partner in the Portland office of K&L Gates LLP, whose practice focuses on complex business litigation, government investigations, and enforcement actions. Although he represents clients in a wide range of industries, John has particular experience serving clients in the renewable energy, transportation, technology, and health care sectors, including health care providers, physicians, insurers, and laboratories. John has represented health care industry clients and government entities in regulatory proceedings, business disputes, and False Claims Act litigation. John has also represented medical professionals and laboratories in fraud investigations. More broadly, John helps clients in a variety of industries respond to inquiries from various state and federal law enforcement and regulatory agencies concerning alleged health care fraud, government contracts fraud, and regulatory and antitrust issues. John regularly manages internal investigations to uncover and manage clients' potential criminal and civil exposure.

Aaron E. Millstein, Author
Aaron Millstein is a partner in the Seattle office of K&L Gates LLP, whose practice focuses on complex commercial litigation, internal investigations, government enforcement, and white collar criminal defense. Aaron has represented clients in numerous industries, with a focus on business disputes and litigation involving a parallel government investigation or proceeding, whether civil or criminal. He has also conducted numerous internal investigations on behalf of corporate clients to address potential legal or ethical violations, such as fraud and theft. With respect to the health care industry specifically, Aaron has represented physicians in negotiations with both state and federal enforcement agencies to resolve allegations of health care fraud, such as violations of the False Claims Act and the Anti-Kickback Statute.

Acknowledgement: Daniel-Charles ("DC") V. Wolf
The authors are grateful to DC Wolf for his substantial contribution to this chapter. Before leaving private practice to serve as a federal judicial clerk, DC was a litigation associate in the Seattle and Chicago offices of K&L Gates LLP.

Chapter Outline:

Editor's Note: This chapter does not discuss the interaction of the HIPAA privacy rule with subpoenas calling for production of patient health information, nor the detailed substantive statutory and regulatory provisions, which, if violated, may give rise to a government investigation. These issues are discussed in a prior version (3rd edition) of the Washington Health Law Manual as follows: Chapter 1A by Mary R. Giannini, Healthcare Information and Confidentiality (2016); Chapter 24 by David B. Robbins et al., Washington State Fraud and Abuse Prohibitions (2010); and Chapter 25 by Charles S. Wright, Antitrust and Consumer Protection Laws (2008).

1 Chapter summary

Government investigations are high-stakes and stressful events for any health care provider. The tools the government uses to conduct its investigations range from formal to informal, but all can create significant risks if not managed properly. For instance, a subpoena or a request for an interview will raise numerous questions. Must a response be provided? What happens if you miss the government's deadline? Do you need to hire outside counsel? May typical recordkeeping practices continue? And, above all, what can health care providers do to be ready to address the government's concerns and reduce the risk of such concerns arising in the future?

This chapter will help readers understand government investigations of health care providers. We begin with an overview of how the government investigates health care fraud and abuse, starting with a discussion of key government agencies, and then describe the tools they use to conduct investigations, ranging from the subtle and informal (e.g., voluntary requests for an informal interview) to the conspicuous and confrontational (e.g., grand jury subpoenas and search warrants).

After that, we discuss best practices for addressing and responding to investigations. This includes the importance of working through experienced counsel, understanding the risks, and approaching key decisions, such as whether to conduct an internal investigation and/or cooperate with the government. We conclude by discussing policies and procedures that health care providers should consider implementing in order to maintain a state of readiness in the event of a government investigation and reduce the likelihood that compliance lapses will occur.[1]

Some key takeaways explored in greater detail below include:

- Consult with experienced outside counsel. The first step in responding to a government investigation should be to consult with experienced outside counsel. Involving counsel at an early stage can help avoid missteps in initial responses to government enforcers, ensure protection of the attorney-client and work product privileges, develop a critical rapport with investigators, and help formulate the best strategy for potential future disclosures or cooperation. Experienced counsel can also assist with conducting an internal investigation to uncover the source and scope of potential problems that led to the investigation in the first place.

- Promptly address and consider objections to subpoenas and other requests for documents. Government subpoenas and civil investigative demands for documents and other information often present significant administrative and logistical burdens, with mandatory response deadlines as short

[1] As described in the editor's note at the beginning of this chapter, we do not address here the intersection of HIPAA, state law confidentiality requirements, and responses to civil investigative demands and subpoenas, nor do we discuss in any detail the statutory and regulatory provisions, which typically underpin a government investigation. These issues are described in other chapters of the Washington Health Law Manual.

as 20 days from receipt. Given the real possibility of good faith errors, and potential penalties for non-compliance, it is important promptly to begin work on an appropriately thorough response. In most instances, the best practice will be promptly to engage with enforcers to raise concerns about unreasonable or overbroad requests and unmanageable deadlines while simultaneously producing more easily available information. Experienced counsel can provide guidance about which requests are objectionable and help negotiate the scope and timing of responses.

- Preserve relevant evidence. When first learning of an investigation, another critical early step is to ensure retention of all potentially relevant documents and evidence. Destruction of relevant evidence, even if inadvertent, may be seen by the government as an attempt to obstruct the investigation, or worse, as an attempt to conceal wrongdoing. To ensure preservation, providers should promptly disseminate document preservation notices to relevant employees and work with IT professionals to suspend any automatic deletion or archiving processes.

- Be deliberate in internal communications about an investigation. What to tell employees about an investigation is driven by the circumstances of each individual case. Generally speaking, however, providers should inform employees about the existence of an investigation, that they are not required to speak with investigators, that they are entitled to consult with an attorney who represents them individually, and that they must tell the truth if they make any statements. Employees should also be instructed how to contact the company's counsel with questions or concerns.

- Conduct an internal investigation. Where it appears a provider is suspected of wrongdoing, a provider should conduct an internal investigation with the assistance of outside counsel. Such an investigation will yield critical information about the scope and severity of the issues that gave rise to the investigation. An investigation conducted by outside counsel will also preserve applicable privileges and provide maximum ability to develop a thoughtful strategy about whether, or the extent to which, the company should cooperate with the government, and the potential benefits and risks of such cooperation.

- Promulgate policies and procedures for responding to government information requests. Providers should establish written policies and procedures for receiving, evaluating, and responding to government inquiries. With respect to written requests like CIDs and subpoenas, the policy should designate a coordinating person to manage responses. The policy should also inform employees of appropriate responses if they are approached by investigators for a surprise interview and how they should respond if government agents execute a search warrant—at a minimum specifying a person to be contacted immediately upon execution of a warrant to ensure coordination of a prompt response. The policy should also direct that counsel be present who can obtain a copy of the warrant, the names and contact information of the agents or officers executing the warrant, a list of everything taken, and a statement from each witness that speaks with government agents.

2 Overview of government investigations

State and federal government agencies and regulatory bodies use a variety of tools to investigate suspected fraud, waste, and abuse; regulatory and statutory violations; or other unlawful practices. The tools used will depend on which agency is investigating, when the investigation begins, and the nature of the matter under investigation.

2.1 Government entities that regulate health care providers

Law enforcement and regulatory agencies at both federal and state levels enforce statutory and administrative regimes that govern the activities of health care providers.

The U.S. Department of Justice ("DOJ") prosecutes criminal health care offenses and brings civil enforcement actions at the federal level. DOJ includes both attorneys in Washington, D.C. ("Main Justice") and attorneys in the 94 U.S. Attorney's Offices throughout the United States. The Main Justice prosecutors are assigned to a dedicated Health Care Fraud Unit within DOJ's Fraud Section.[2] DOJ conducts investigations through the Federal Bureau of Investigation, the U.S. Department of Health and Human Services ("HHS") Office of the Inspector General ("OIG"), the Food and Drug Administration, the Drug Enforcement Administration ("DEA"), state attorneys general, and state law enforcement agencies.

DOJ enforces a variety of statutes prohibiting fraud, theft, and embezzlement in the health care industry, including the submission to the government of false claims for payment.[3] DOJ also investigates violations of statutes aimed at protecting consumers from dangerous or mislabeled drugs and devices[4] or conflicts of interest that could compromise patient care or incentivize overbilling (such as the Stark Law and the Anti-Kickback Statute).[5] DOJ also prosecutes violations of the federal criminal health care fraud statute. Criminal charges not specific to the health care industry—such as wire or mail fraud, making false statements to federal agents, conspiracy, and obstruction of justice—also commonly arise in cases involving health care providers.

Within the HHS, the Centers for Medicare and Medicaid Services ("CMS") administers Medicare and works with states to administer Medicaid and the Children's Health Insurance Program.[6] CMS conducts administrative proceedings related to contested audits, billing disputes, and claim denials. CMS also works closely with DOJ and with the OIG to investigate fraud, waste, and abuse in government health care programs.[7] OIG will refer suspected criminal violations to DOJ or to state Medicaid fraud units for prosecution. While OIG does not file criminal charges, its OIG special agents have law enforcement authority and investigate criminal and civil health care cases at DOJ's direction. OIG also can levy monetary penalties and order a provider's exclusion from federal health care programs.[8]

Because the states administer Medicaid, each state, along with the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, has a Medicaid Fraud Control Unit ("MFCU") that is independent from the state's Medicaid program. MFCUs work with state law enforcement to investigate and prosecute fraud and abuse in the state Medicaid program. HHS OIG oversees and evaluates the MFCUs, which

---

[2] A useful description of the Health Care Fraud Unit is found here: https://www.justice.gov/criminal-fraud/health-care-fraud-unit.

[3] *See* Robbins et al., *supra* note 1, §§ 24.2.1, 24.2.3.

[4] *See, e.g.*, *80 Years of the Federal Food, Drug and Cosmetic Act*, FDA.GOV (July 11, 2018), https://www.fda.gov/about-fda/fda-history-exhibits/80-years-federal-food-drug-and-cosmetic-act.

[5] *See* Robbins et al., *supra* note 1, §§ 24.2.2, 24.2.4 (describing the Anti-Kickback Statute and the Stark Law).

[6] *See generally* Vickie J. Williams, *Government Payors of Medical Services*, *in* WASH. HEALTH L. MANUAL Ch. 20 (3d ed.).

[7] *See* Williams, *supra* note 6, §§ 20.2.6, 20.4.7.

[8] *See* Robbins et al., *supra* note 1, § 24.2.6.

receive a portion of their funding from federal grants.[9] State Medicaid programs also conduct their own audits of providers to ensure compliance with program rules.[10]

In addition to their roles in policing Medicaid programs, state regulatory and law enforcement officials—usually working in a state department of health, medical board, or attorney general's office—regulate health care providers through licensing and credentialing regimes and by enforcing statutory and regulatory frameworks analogous to those DOJ enforces at the federal level.[11]

Private-sector entities also play an important role. For example, while CMS administers Medicare, it contracts to private insurance companies and auditing firms the processing, payment, and review of Medicare claims. These contractors work to identify billing practices that could lead to waste or indicate abuse of program resources. They also conduct audits and investigations, take certain administrative actions, and refer cases to law enforcement for prosecution.[12]

Private plaintiffs called "relators" also play a role in regulating health care providers by filing *qui tam* lawsuits under the civil False Claims Act and its state-law analogues. Such statutes authorize private parties to file lawsuits on the government's behalf and, in return, share in a portion of any monetary recoveries. Relators must file *qui tam* lawsuits under seal and serve a copy of the lawsuit on DOJ.[13] DOJ then investigates the allegations and may decide to intervene in the case, effectively taking over the private lawsuit and turning it into a civil enforcement action.[14] If the government declines to intervene, the relator typically may proceed to prosecute the litigation without the government's assistance.[15] The government also has the power to dismiss the case, and it will do so in limited circumstances, such as where the claim is factually baseless or contrary to government policy.[16]

2.2 How government investigations begin

Most of the investigative techniques discussed in this chapter are overt—that is, the government acknowledges that an investigation exists by asking for an interview, issuing a subpoena or Civil Investigative Demand ("CID"), or executing a search warrant at an office, home, or elsewhere. But investigations often begin—in a variety of ways—before (sometimes long before) their existence is apparent. For example, authorities may receive information from criminal defendants seeking leniency, from an informal whistleblower report, or from a relator whistleblower's filing of a *qui tam* lawsuit. Information received from the private sector through routine contact with regulators (e.g., audits or securities filings) can also lead to an investigation. Similarly, news reports, current events, and prevailing social or political attitudes can invite regulatory scrutiny on particular industries, companies, or practices. DOJ also has become very sophisticated and aggressive in terms of using data analytics to

---

[9] *Medicaid Fraud Control Units*, U.S. DEP'T OF HEALTH & HUM. SERVS. OFF. OF INSPECTOR GEN., https://oig.hhs.gov/fraud/medicaid-fraud-control-units-mfcu/ (last visited Sept. 21, 2021).

[10] *See* Williams, *supra* note 6, § 20.4.7.

[11] *See* Robbins et al., *supra* note 1, § 24.3; Donna Moniz & Michelle Taft, *Professional Licensure of Individuals*, *in* WASH. HEALTH L. MANUAL Ch. 9 (3d ed., 2015); Chris Marsh & Kyran Hynes, *Hospital Regulation*, *in* WASH. HEALTH L. MANUAL Ch. 10 (3d ed. 2015).

[12] *See* Williams, *supra* note 6, § 20.4.7.

[13] *See* 31 U.S.C. § 3730(b)(2).

[14] *Id.* § 3730(b)(4).

[15] *Id.* § 3730(c)(3).

[16] *Id.* § 3730(c)(2); *see generally* U.S. Dep't of Just., Just. Manual § 4-4.111 (2018) (discussing grounds for government to dismiss a qui tam case).

identify and target suspicious billing levels and patterns, emerging schemes, and schemes that cross geographical boundaries.

Once initiated, investigations often continue in secret before the government starts using overt investigative tactics. For example, wiretaps—once reserved for organized crime, narcotics, and national security cases—are now often used to investigate white-collar criminal offenses,[17] including those involving health care providers.[18] The government can execute search warrants for personal email or social media accounts without prior notice to the account holder. The government also may use physical surveillance and confidential informants to investigate covertly. The goal of covert techniques such as these is to obtain unfiltered, spontaneous, truthful admissions or information about otherwise secret activities. The government can also use covertly obtained evidence as grounds for perjury or obstruction charges if that evidence contradicts what someone tells the government in response to an overt request (like an interview or subpoena).

2.3 Government investigative tools

At some point the government may openly seek information from the persons it is investigating. The following sections summarize the tools the government uses: (1) surprise interviews, (2) informal requests for documents or interview, (3) preservation notices, (4) CIDs, (5) subpoenas, and (6) search warrants.

2.3.1 "Knock-and-talk"/Surprise interviews

An often-used tactic of law enforcement agents and regulatory investigators is making unscheduled requests for an impromptu interviews on an unsuspecting employee. In a so-called "knock and talk," for example, agents will come to the employee's home, ring the doorbell, and ask for an informal conversation. These visits frequently occur at 6:00 a.m. or 7:00 a.m., often before you have finished your first cup of coffee. Investigators might also appear at a company facility and use the same tactic. Whether at home or in the office, the goal is to catch the interviewee off guard and obtain unguarded admissions.

This dynamic creates a fraught scenario. An employee may be inclined to talk to agents, thinking that it will be possible to withhold key information while learning about the investigation and alleviating the government's concerns. Employees may also believe that they have no choice but to comply with an agent's request. But it is not obstruction of justice to decline an agent's request for an interview. Indeed, as explained below (*see* Sec. 3.1), the best practice is to not grant an initial request for an interview, but rather to confer with counsel about whether an interview is advisable under the circumstances and, if so, how to properly prepare for it.

---

[17] *See* Jordan Maglich, *Once Reserved for Drug Crimes, Wiretapping Takes Center Stage in White Collar Prosecutions*, FORBES (May 21, 2013), https://www.forbes.com/sites/jordanmaglich/2013/05/21/once-reserved-for-drug-crimes-wiretapping-takes-center-stage-in-white-collar-prosecutions/?sh=459a4f319691.

[18] *See, e.g.*, United States v. Poulsen, 655 F.3d 492, 505 (6th Cir. 2011) (affirming denial of motion to suppress evidence obtained from a wiretap in prosecution of health care finance company CEO for scheme to defraud purchasers of bonds backed by health care providers' accounts receivable); United States v. Zemlyansky, 945 F. Supp. 2d 438, 481–83 (S.D.N.Y. 2013) (denying motion to suppress wiretap evidence in health care fraud prosecution of operators of insurance billing scheme).

2.3.2 Informal requests for information

One step removed from a "knock and talk" visit is an informal request to provide an interview or documents at some future time. The difference here is that, rather springing an impromptu request, agents make contact by phone or letter and ask to schedule an interview or a document production.

As with surprise interview requests, these informal requests are entirely voluntary. But health care providers must take such inquiries seriously. A health care provider's response to an informal request for information can set the tone for future interactions with investigators and may be a chance to begin that process in a cooperative, nonadversarial manner (although such interactions should still occur through counsel—*see* Sec. 3.1). Moreover, a voluntary information request may not truly be "voluntary." For example, certain Washington state statutory or administrative provisions provide that failure to cooperate can result in licensing, disciplinary, or other repercussions if the recipient of the inquiry is a medical professional.[19] Similarly, denying or ignoring a request from HHS OIG can lead to temporary or permanent exclusion from government health programs.[20] Ignoring or rejecting an informal request can also prompt further scrutiny by making it look as though the recipient has something to hide.

2.3.3 Document preservation notice

Civil enforcement authorities sometimes issue demands that the recipient preserve specified documents. Doing so signals the government's belief that the recipient of the notice possesses records that are potentially relevant to a contemplated or ongoing investigation. Receiving such a notice may also mean that a formal subpoena is forthcoming.

Preservation notices are "voluntary" insofar as the government cannot force someone to preserve documents merely by issuing a preservation notice. However, the recipient of a preservation notice should comply with it. If the government later serves a subpoena, even the innocent destruction of documents after issuance of a preservation notice may be deemed spoliation of evidence. The government may also see failure to preserve documents as independent evidence of wrongdoing or, even worse, as the criminal offense of obstruction of justice.[21]

2.3.4 Civil investigative demand

Federal and state law enforcement agencies are authorized to issue CIDs requiring production of information relevant to civil enforcement investigations. Though similar to subpoenas (*see*

---

[19] *See, e.g.*, RCW 18.130.180(8) (Uniform Disciplinary Act for Regulation of Health Professions defining as "unprofessional conduct" the failure of any license holder to "cooperate with the disciplining authority" by not providing requested records, written explanations, or the like).

[20] *See* 42 U.S.C. § 1320a-7(b)(12) (authorizing the secretary of HHS to exclude from "any federal healthcare program . . . [a]ny individual or entity that fails to grant immediate access, upon reasonable request, to" certain federal and state regulatory authorities charged with investigating and prosecuting fraud in federal health care programs).

[21] 18 U.S.C. § 1519 ("Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.")

Sec. 2.2.5), CIDs differ in that they allow investigators to propound written interrogatories in addition to seeking documents and testimony.[22]

Both DOJ[23] and the Washington State Attorney General's Office[24] use CIDs to investigate suspected civil violations of federal and state false claims acts. While CIDs are restricted to civil proceedings, civil authorities may share information produced in response with criminal prosecutors.[25] Both the federal and state CID statutes also allow the government to share information obtained through a CID with *qui tam* relators—i.e., private plaintiffs in false claims cases—if doing so is determined to be necessary as part of a false claims investigation.[26]

Complying with a CID is mandatory. Should a recipient fail to comply, an investigating agency can enforce a CID through a civil lawsuit. The discovery provisions of the applicable rules of civil procedure (i.e., the Federal Rules of Civil Procedure or the Washington Superior Court Civil Rules) will govern enforcement of the CID.[27] This does not mean, however, that the recipient of a CID can "conduct routine discovery [from the government] as if the petition [to enforce the CID] were a civil action," because "Congress intended to make the Federal Rules of Civil Procedure available to the CID recipient for use as a shield, not as a sword."[28]

2.3.5 Subpoenas

From the Latin *sub poena*, meaning "under penalty," a subpoena is a mandatory, judicially enforceable order to produce documents, provide testimony, or appear for a judicial or administrative proceeding. Though there are various types of subpoenas, the most commonly used type in government investigations of health care providers are administrative subpoenas and grand jury subpoenas.

---

[22] *See* 31 U.S.C. § 3733(a)(1)(B) (authorizing written interrogatories); RCW 74.66.120(1)(a)(ii) (same).

[23] *See* 31 U.S.C. § 3733(a)(1).

[24] *See* RCW 74.66.120(1)(a).

[25] *See* 31 U.S.C. § 3733(i)(2)(B) (authorizing the creation of copies of materials produced in response to a CID "as may be required for official use by any false claims law investigator or other employee of the Department of Justice"); RCW 74.66.120(21)(b) (authorizing copies "as may be required for official use by any false claims act investigator, or employee of the attorney general"); 31 U.S.C. § 3733(i)(3) (authorizing a false claims investigator designated by DOJ as custodian of materials provided in a response to a CID to deliver such materials to "any attorney of the Department of Justice" who "has been designated to appear before any court, grant jury, or Federal agency in any case or proceeding, . . . for official use in connection with any such . . . proceeding as such attorney determines to be required"); RCW 74.66.120(22) (same, with respect to "any official" who "has been designated to appear before any court, special inquiry judge, or state administrative proceeding").

[26] 31 U.S.C. § 3733(a)(1)(D); RCW 74.66.120(1)(b).

[27] *See* 31 U.S.C. § 3733(b)(1)(B) (CIDs "may not require" the recipient to provide information if it would be protected from disclosure under, among other things, "[t]he standards applicable to discovery requests under the Federal Rules of Civil Procedure," but then, only "to the extent that the application of such standards to any such demand is appropriate and consistent with the provisions and purposes of this section."); RCW 74.66.120(3)(b) (same with respect to Washington CIDs and the superior court civil rules); 31 U.S.C. § 3733(j)(6) (Federal Rules of Civil Procedure govern enforcement actions); RCW 74.66.120(30) (superior court civil rules govern enforcement actions).

[28] United States v. Witmer, 835 F. Supp. 201, 205 (M.D. Pa. 1993), *vacated in part upon reconsideration on other grounds*, 835 F. Supp. 208 (M.D. Pa. 1993).

2.3.5.1 *Administrative subpoenas*

Although numerous federal agencies have subpoena power,[29] the so-called "HIPAA subpoena" is most relevant to government investigations of health care providers. Enacted as part of the Health Insurance Portability and Accountability Act ("HIPAA"), 18 U.S.C. § 3486(a)(1)(A)(i)(I) authorizes DOJ to issue subpoenas "[i]n an investigation of a Federal health care offense."

A HIPPA subpoena is narrower in scope than a CID in that a HIPAA subpoena may only compel document productions and can only compel testimony from the custodian of the documents to establish chain of custody or authenticity.[30] Unlike a CID, a HIPAA subpoena cannot seek written interrogatory responses or free-ranging testimony. Still, a HIPAA subpoena could signal higher stakes compared to a CID: It signals the existence of a criminal investigation; it allows the government to seek an *ex parte* gag order preventing disclosure of the existence of the subpoena for 90 days (if necessary to prevent specified harms);[31] and the enabling statute expressly provides that failure to comply with a HIPAA subpoena may subject the recipient to contempt-of-court proceedings.[32]

Both DOJ criminal and civil prosecutors may use evidence produced in response to a HIPAA subpoena.[33] A HIPAA subpoena may thus signal not just a criminal investigation, but also the existence of a parallel civil investigation.

In addition to HIPAA subpoenas, the DOJ can issue administrative subpoenas for both documents *and* witness testimony "[i]n any investigation relating to his [the Attorney General's] functions . . . with respect to controlled substances, listed chemicals, or encapsulating machines."[34] The U.S. Attorney General has delegated this subpoena authority to the DEA.[35] DEA subpoenas are not limited to enforcing the civil regulatory provisions of the Controlled Substances Act; they can also be used in criminal investigations.[36]

Lastly, the Inspector General Act of 1978 authorizes inspectors general to issue subpoenas for information needed in administrative, civil, and criminal investigations.[37]

---

[29] *See, e.g.*, U.S. DEP'T OF JUST., OFF. OF LEGAL POL'Y, REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES, https://www.justice.gov/archive/olp/rpt_to_congress.htm [hereinafter DOJ Subpoena Report].

[30] 18 U.S.C. § 3486(a)(1)(B)(i)–(ii).

[31] *Id.* § 3486(a)(6)(A)–(B) (to obtain an ex parte gag order, the government must show that disclosure of the subpoena's existence "may result in" (i) danger to life or physical safety, (ii) flight from prosecution, (iii) the loss of evidence; or (iv) the intimidation of potential witnesses).

[32] *Id.* § 3486(c).

[33] DOJ Subpoena Report, *supra* note 29, at Sec. III.A.

[34] 21 U.S.C. § 876(a).

[35] United States v. Harrington, 761 F.2d 1482, 1485 (11th Cir. 1985).

[36] *Id.*; *see also* United States v. Mountain States Tel. & Tel. Co., 516 F. Supp. 225, 229 (D. Wyo. 1981); United States v. Hossbach, 518 F. Supp. 759, 765 (E.D. Pa. 1980).

[37] DOJ Subpoena Report, *supra* note 29, at Sec. II.B.1; 5 U.S.C. app. 3 § 6.

These subpoenas are limited to requiring production of documents.[38] OIG can share what it receives in response to such subpoenas with DOJ personnel investigating both civil and criminal matters.[39] The OIG has broad authority to investigate waste, fraud, and abuse in various federal agencies, departments, and programs.[40] Thus, compared to a CID (used in False Claims Act investigations), a HIPAA subpoena (used in criminal health care investigations), or a grand jury subpoena (used by grand juries to investigate whether to authorize criminal charges), it may be harder for the recipient of an OIG subpoena to determine the nature of the investigation and whether or not the DOJ is involved, because an OIG can issue a subpoena in furtherance of any of its investigative functions.[41]

Compliance with administrative subpoenas is mandatory. If the subpoena recipient refuses to comply, the government may bring an enforcement action in federal court to force compliance under penalty of the court's contempt powers.

2.3.5.2 *Federal grand jury subpoenas*

A federal grand jury subpoena is a compulsory order to provide documents or testimony deemed by a DOJ criminal prosecutor to be relevant to a federal grand jury investigation. Grand juries are a constitutionally established part of the federal criminal justice system.[42] Although Washington state law authorizes courts to convene grand juries,[43] grand juries are rarely used in Washington state prosecutions.[44] This section thus focuses on federal grand jury investigations.

A grand jury is an independent body of private citizens that investigates (under the guidance and direction of criminal prosecutors) suspected crimes, initiates federal criminal prosecutions, and serves as a theoretical check on the government's prosecutorial authority.[45] The grand jury's ultimate purpose is to decide whether there is probable cause to believe that someone committed a criminal offense; if there is, the grand jury can return an indictment. Grand juries can subpoena records and testimony to aid them in making this decision.

---

[38] 5 U.S.C. app. 3 § 6(a)(4).

[39] *See, e.g.*, 5 U.S.C. app. 3 § 4(d) (requiring inspectors general to "report expeditiously to the Attorney General whenever the Inspector General has reasonable grounds to believe there has been a violation of Federal criminal law").

[40] *See id.* app. 3 §§ 2, 12(2).

[41] Brian M. Feldman, *Navigating Federal Anti-Fraud Subpoenas*, 247 N.Y.L.J. NO. 12 (Jan. 19, 2012), https://www.hselaw.com/files/navigating_anti_fraud_subpoenas.pdf; *see also* 5 U.S.C. app. 3 § 6(a)(4).

[42] U.S. Const. amend. V ("No person shall be held to answer for a capital or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury . . . ."). *But see* Hurtado v. California, 110 U.S. 516 (1884) (holding that the Fifth Amendment does not require grand juries in state criminal prosecutions).

[43] *See generally* Ch. 10.27 RCW.

[44] *See* Beck v. Washington, 369 U.S. 541, 545 (1962) ("The grand jury in this case, the eighth called in King County in 40 years, was summoned primarily to investigate circumstances which had been the subject of the Senate Committee hearings.").

[45] *See* Fed. R. Crim. P. 6; U.S. Dep't of Just., Justice Manual 9-11.010 (2020).

Strict rules of secrecy cloak grand jury proceedings from disclosure.[46] Thus, unlike the investigative tools discussed above, outside of narrow circumstances, criminal prosecutors *cannot* share information related to grand jury proceedings and subpoenas with other government lawyers or investigators.[47]

DOJ uses three designations to describe the status of persons of interest to the grand jury. A **target** is someone "as to whom the prosecutor or the grand jury has substantial evidence linking him or her to the commission of a crime and who, in the judgment of the prosecutor, is a putative defendant."[48] A **witness** is any person that possesses evidence or has knowledge that the government believes may be relevant to its investigation. A person can be a witness without observing or being involved in a crime; compared to being designated a target, being classified as witness portends relatively less risk of criminal exposure. Situated between a target and a witness in terms of the risk of possible criminal charges, a **subject** is someone "whose conduct is within the scope of the grand jury's investigation."[49]

DOJ uses these designations to classify people with information relevant to an investigation even if a grand jury is not involved. Although it is significant to learn if the government has classified you as a target versus a witness or a subject, the latter two labels can have limited utility. One's status as a witness or subject may change as an investigation progresses (for instance, if someone classified as a witness lies to investigators), making it important to tread carefully even if the government informs you that you are not a target.

Complying with a grand jury subpoena is mandatory, and failure to do so is punishable by contempt of court.[50] However, because grand juries investigate crimes, receiving a grand jury subpoena—particularly one seeking oral testimony—may, under certain circumstances, implicate the Fifth Amendment rights of the subpoena recipient, freeing that witness from compelled self-incrimination if the witness decides to invoke his or her Fifth Amendment right (or "Take the Fifth").

When a health care provider responds to a CID or a subpoena, it is often wise to engage experienced outside legal counsel to provide advice on the provider's rights and responsibilities, including an assessment of whether the CID or subpoena is more broadly drafted than is permitted by law and whether the CID or subpoena calls for information that enjoys legal protection, including but not limited to the attorney-client privilege. It is imperative that communications with legal counsel on these topics be clearly labeled as "confidential" and "attorney-client privileged."

2.3.6 Execution of a search warrant

The government's most powerful—and often most conspicuous—investigative tool is the search warrant. To obtain a search warrant, the government must persuade a judge that a crime has

[46] Fed. R. Crim. P. 6(e)(2).

[47] *See id.* 6(e)(3)(A)–(B).

[48] U.S. Dep't of Just., Justice Manual 9-11.151 (2020).

[49] *Id.*

[50] Fed. R. Crim. P. 17(g); U.S. Dep't Justice Manual 9-11.140 (2018).

occurred and that there is probable cause to believe that evidence of that crime will be found in a particular location.[51] If the judge agrees, he or she will issue a warrant, authorizing the government to search for and seize the evidence specified in the warrant.

Cooperation with a search warrant is mandatory, and knowingly interfering with the execution of a warrant is a crime.[52] In addition, law enforcement agents are authorized to use force to the extent reasonably necessary to execute the warrant.

Of particular relevance to health care providers, DOJ regulations state that search warrants should not ordinarily be used to obtain records from a physician if the records contain confidential patient information.[53] An exception exists if it appears that records of substantial importance to the investigation cannot be obtained through less-intrusive means, and DOJ leadership must approve the warrant application where that is the case.[54] This policy applies to records created by a physician "but retained by the physician as a matter of practice at a hospital or clinic," unless "the clinic or hospital is a suspect in the offense."[55] Also, agents executing a warrant that authorizes them to search for sensitive patient information must do so "in such a manner as to minimize, to the greatest extent practicable, scrutiny of confidential materials."[56] Notwithstanding these regulations and policies, government agents cannot be relied upon to scrupulously know of or follow these regulations, and they certainly cannot be relied upon to act in a health care provider's best interest on these subjects when drafting an affidavit in support of a search warrant or when executing a search warrant. For example, in May 2017, DOJ executed search warrants at five different offices and locations of a health care provider in Texas.[57] The information used to supply the probable cause needed for the search warrants came from allegations in two *qui tam* lawsuits, from evidence that HHS OIG obtained after issuing requests for information concerning the allegations in *qui tam* lawsuits, and from evidence DOJ obtained after issuing CIDs.[58] The government seized 29 smartphones, 20 computers and hard drives, and the email accounts of 17 employees, including the provider's Director of Compliance.[59] During the search, the government seized thousands of documents and emails that constituted privileged communications between the Director of Compliance and the provider's outside counsel.[60] The provider filed a motion for the return of the privileged material under Rule 41(g) of the Federal Rules of Criminal Procedure, which the district court denied, and the provider appealed.[61] The Fifth Circuit Court of Appeals held that the government had acted in "callous disregard" of the

---

[51] *See* U.S. Const. amend. IV.

[52] *See, e.g.*, 18 U.S.C. § 1501 ("Whoever knowingly and willfully obstructs, resists, or opposes any officer of the United States or any other person duly authorized, in serving, or attempting to execute, any legal or judicial writ or process" shall be fined or imprisoned).

[53] 28 C.F.R. § 59.4(b)(1)–(2).

[54] *Id.*

[55] *Id.* § 59.4(b)(1), n.2.

[56] *Id.* § 59.4(b)(4).

[57] *See* Harbor Health Sys., L.P. v. United States, 5 F.4th 593, 596 (5th Cir. 2021).

[58] *Id.* at 595.

[59] *Id.* at 596.

[60] *Id.* at 596–97.

[61] *Id.*

provider's rights and that the district court had incorrectly concluded otherwise, and it remanded the case back to the district court.[62]

Agents executing a warrant will often ask to interview employees who are present during the search. (*See* Sec. 2.3.1). Such a request uses the surprise and disarray of the search warrant process to obtain unguarded statements from potential witnesses. This can be a stressful, even frightening, experience for employees and staff. As described below (*see* Sec. 4.1), establishing clear policies to guide personnel during a search warrant execution well before one happens helps reduce unnecessary contact with government agents and minimize disruption to company operations.

3 Best practices for responding to a request or demand for information.

3.1 Retaining experienced counsel.

3.1.1 In general.

Regardless of how the government first makes contact or seeks information, the prudent course is to identify and consult with counsel and, if possible, ensure appropriate internal messaging to employees, before providing a substantive response. Although a health care provider might be inclined to rely on in-house legal personnel for this, the better course is to retain outside counsel. Government investigations are critically different from matters that in-house legal departments typically handle, such as responding to private subpoenas issued in civil lawsuits,[63] overseeing transactional matters, or liaising with regulators for routine auditing or compliance duties. As such, health care providers should engage counsel with experience in government investigations.

There are considerable benefits to working through counsel rather than dealing directly with the government. First, doing so will reduce the risk of costly missteps that can occur when speaking with investigators. (*See* Sec. 3.2). Second, initial impressions are key. The government wants to know if it is dealing with someone who will be straightforward and take the inquiry seriously or will "hide the ball" or be dilatory or obstructionist. An attorney accustomed to communicating with law enforcement will understand the importance of rapport-building and credibility, as well as how to cultivate these when dealing with the government. Communications with government investigators differ markedly from those in private civil litigation, where lawyers often resist discovery, raise objections, and dispute the validity of the request. Third, working through an attorney provides an added protection via the attorney-client privilege, which will safeguard conversations between lawyer and client about the investigation or about the lawyer's interactions with the investigators.

After the health care provider retains counsel (for itself and/or for one or more employees), the attorney should contact the investigating agents to explain that the clients have retained counsel who will handle further communications with the government. The initial call with investigators can be an opportunity for counsel to begin building rapport with the investigators and potentially gain insights about the investigation. Counsel also may be able to negotiate the scope of the

[62] *Id.* at 599–601.

[63] *See* Fed. R. Civ. P. 45.

government's request and the timing of a response, which can provide time for additional preparation[64] and can mitigate the burdens of responding.

3.1.2 Retaining counsel for individual employees.

Government investigators may direct a CID or administrative subpoena not just to a health care provider, but also (or instead) to one or more employees. In such instances, the health care provider should consider whether to provide legal counsel for the employee.[65] If the employee's and the employer's interests are adverse to one another (for example, if the employee is suspected of wrongdoing), the employee may need separate counsel. If one or more employees are similarly situated, however, retaining a single attorney to act as "pool counsel" for those potential witnesses may be an option.[66] Even if the company decides not to provide counsel for its employees, the company should still inform employees about the risks of responding to the government, the advisability of consulting with a lawyer, and that employees who receive investigative inquiries inform the company when this happens.

The same principles apply where the government requests on-site access to records or attempts to spring surprise interviews on employees. The same attorney can represent similarly situated employees, though separate counsel is likely necessary if the employee or employees may be independently culpable or otherwise have interests adverse to the employer's or to other employees.

DOJ policy instructs prosecutors not to consider whether a company is paying employees' legal fees when assessing the adequacy of the company's cooperation.[67] Prosecutors also are not supposed to tell companies not to pay employees' legal fees, but that does not prevent prosecutors from asking about "the representation status of a corporation and its employees, including how and by whom attorneys' fees are paid."[68] The Justice Manual cautions, however, that criminal obstruction of justice statutes still apply, for example, if a company promises to advance legal fees in exchange for the employee making false statements.[69]

3.2 Ensuring appropriate internal communication regarding the investigation.

Health care providers must also decide what to tell employees about the investigation. There is no one-size-fits-all approach to this issue. What to tell employees will depend on the facts and dynamics of each particular case. But at a minimum, the employer should alert employees about the existence of an investigation, their legal rights, the possibility that the government could contact them, and whom to

[64] Depending on the nature of the government's inquiry, there may be pressing deadlines of which to be aware. For example, a health care provider that has identified an overpayment from Medicare or Medicaid, or who should have done so "through the exercise of reasonable diligence," has 60 days to report the overpayment to CMS. *See* 42 C.F.R. 401.305(a)–(b). Knowingly failing to report can result in DHHS OIG imposing administrative penalties.

[65] In some instances, organizational bylaws or employment agreements could require the employer to indemnify the employee or reimburse the employee for certain legal fees.

[66] *See, e.g.*, *Representing Multiple Individuals in the Context of a Governmental or Internal Investigation*, N.Y.C. Bar, Comm. on Pro. Ethics, Formal Op. 2019-4 (May 16, 2019), https://s3.amazonaws.com/documents.nycbar.org/files/2019529-Pool_Counsel_FINAL.pdf.

[67] Justice Manual 9-28.730.B.

[68] Justice Manual 9-28.370.B n.1.

[69] Justice Manual 9-28.730.B.

contact (the company's attorney) if that happens or if the employee has questions or concerns. This advance notification can help avoid unforced errors, reducing the risk that surprised, overconfident, or underinformed employees could spread misleading rumors or make inaccurate statements to the government.

Communicating with government agents can be perilous. Whether conducting a knock-and-talk, leaving a voicemail, or asking to chat during a search, law enforcement agents often will not remind employees that agreeing to talk is optional or that they are entitled to have an attorney present during questioning. Worse, most people are unaware that lying to a federal agent during an interview is a crime.[70] If an employee tells investigators something that is not true, there might be a dispute over whether it was a deliberate lie or an innocent oversight. Even if the government does not charge someone with making false statements to investigators, such missteps can irreparably shape the government's perception of the interviewee, who might have incorrectly assumed that an informal, preliminary talk with agents is somehow different from a formal on-the-record interview. From the government's point of view, there is no difference. Further complicating matters, it is well established that federal agents are permitted to mislead or deceive a witness during an interview and to audio and/or video-record the interview without notifying the witness.

As such, it is vitally important to notify employees of their rights and obligations when it comes to interacting with the government. A memorandum to employees or company policy on these issues should contain, at least, the following information:

- Whether to talk to investigators is for each employee to decide for themselves. Declining to be interviewed is not obstruction of justice, and employees should feel free to politely decline to be interviewed or direct the investigators to the witness's legal counsel if available.
- Employees are entitled to consult with a lawyer before agreeing to an interview and to have the lawyer present for the interview.
- If an employee decides to talk to the government, the employee must tell the truth.
- Employees should contact the company's counsel with any questions or concerns.
- Employees should also contact the company's counsel if government investigators contact them asking about the company or if the employee decides to talk to the investigators.

It is important to get these instructions right. Health care providers must refrain from doing anything to impede a government investigation, as prosecutors consider "whether the corporation has engaged in conduct intended to impede the investigation" in assessing whether to bring criminal charges.[71] "[I]nappropriate directions to employees or their counsel, such as directions not to be truthful or to conceal relevant facts; making representations or submissions that contain misleading assertions or material omissions; and incomplete or delayed production of records" are all examples of conduct that could prompt prosecutors to look unfavorably on a health care provider's conduct.[72] Depending on the circumstances, efforts to prevent employees from speaking to the government, or to encourage them to lie under oath, could even lead to independent criminal charges for obstruction of justice or perjury.[73]

Health care providers should also advise employees, especially those in leadership and supervisory positions, about legal protections for whistleblowers. If there is a known whistleblower or informer, for

[70] 18 U.S.C. § 1001.

[71] Justice Manual 9-28.730.

[72] *Id.*

[73] *See, e.g.*, 18 U.S.C. §§ 1505, 1510, 1518, 1621, 1622, 1623.

example, in a *qui tam* case under the civil False Claims Act, employers could face civil and, potentially, criminal liability[74] for taking adverse employment actions, or otherwise retaliating, against employees because of the employee's cooperation with the government or due to "lawful acts done . . . in furtherance of" a False Claims Act *qui tam* action.[75]

3.3 Preserving and collecting documents

Upon receiving a preservation notice, a CID, or a subpoena (or even an informal request for information), a health care provider should implement appropriate document retention protocols and issue a notice instructing certain employees and information technology (IT) personnel to suspend any routine document destruction practices. An attorney can draft a preservation memo to be distributed to employees and can coordinate directly with IT professionals to implement the preservation measures.

The health care provider should work with counsel to determine how best to collect what the government has requested. Having counsel work with the employer's IT department to collect the relevant documents is generally preferable to relying on employees themselves to decide which of their documents to preserve and collect. Having counsel collect documents can also help build credibility with the government by ensuring a comprehensive document collection and avoiding the risk or the perception that materials are being withheld. Additional effort may be required in instances where employees use personal electronic devices for work-related communications. While collecting information from such devices may seem intrusive and is not always necessary, it is often required, and doing so will ensure comprehensiveness and enhance credibility.

Failure to preserve documents relevant to an ongoing investigation can have serious consequences. These include judicially imposed sanctions such as fines, fee awards, and instructing the jury to infer that the lost evidence would have been harmful to the person who failed to preserve it. If evidence was knowingly destroyed or hidden, that could be grounds for criminal charges for obstruction of justice.[76] Failing to preserve documents can also result in the loss of helpful or exculpatory materials that could have been useful in negotiating with the government or mounting a defense.

3.4 Conducting an internal investigation

A health care provider might be unaware of law enforcement's or a regulatory agency's concerns until the provider receives a subpoena or a request for information or until the government executes a search warrant. While the cause, nature, and focus of the government's investigation may be unclear at first, the content of the government's request, the requesting agency, and conversations with the investigators can often provide meaningful clues about these important considerations. In other instances, a health care provider might learn of questionable conduct before the government issues any investigative demand.

In either scenario, health care providers should consider whether to conduct their own internal investigation. There are several potential reasons for doing so. An internal investigation can potentially:

- Uncover the truth and get ahead of the facts, which permit an assessment of potential legal risks and can inform decisions about whether and in what manner to cooperate with the government.

[74] *See id.*

[75] 31 U.S.C. § 3730(h).

[76] *See, e.g.*, 18 U.S.C. §§ 1518, 1519.

- Demonstrate the health care provider's commitment to identifying and remedying compliance issues.
- If conducted in a thorough, procedurally sound, and independent manner, be relevant to the government's decision about whether to pursue criminal charges. (*See* Sec. 3.5.1).
- Help the health care provider take appropriate action to address questionable conduct, perhaps by disclosing it to the government, disciplining wrongdoers, or taking other remedial action.
- Help identify practices or policies that need improvement.

If a health care provider decides to conduct an internal investigation, it must also decide how to conduct the investigation. Two considerations are particularly important.

First, the method used to conduct an internal investigation directly influences the perceived reliability and integrity of any conclusions that it reaches. Having a company's in-house legal department conduct the investigation, for example, risks creating the appearance that the investigation was not truly "independent." As such, the safest practice is to retain a reputable outside firm to conduct the investigation. Likewise, management and outside counsel should establish clear rules governing the frequency and nature of communication between management and the law firm while the investigation is in progress.

Second, the investigation must be conducted in a manner best suited to protect the attorney-client privilege. A law firm conducting an investigation represents the company that retained the firm; as such, any investigative report (whether written or given verbally) is typically (but not necessarily) subject to the attorney-client privilege, as are communications between counsel and the client's employees that occur for purposes of conducting the investigation. Because the client holds the privilege, a health care provider retaining a firm to conduct an investigation should work with counsel to ensure confidentiality safeguards to preserve the privilege. This includes, for example, providing the warning contemplated in *Upjohn Co. v. United States*, 499 U.S. 383 (1981), when interviewing company personnel, i.e., that the investigating lawyer represents the company and not the employee in his or her personal capacity, that only the company can decide whether and under what circumstances to waive the privilege, and the company may decide to do so and disclose to the government or to third parties any information the employee provides to the investigating lawyer.

The mere fact that an attorney prepares an investigative report or interview notes does not make the materials privileged; whether the privilege protects investigatory materials generated from an internal investigation instead depends in part on whether the company began the investigation for the primary purpose of obtaining legal advice.[77] Likewise, privilege will not apply unless the communication is intended to be confidential. That might not be the case if someone is talking to an investigating lawyer with the understanding that the lawyers are collecting information to disclose to third parties, such as outside auditors.[78] The attorney-client privilege also does not prevent disclosure of underlying facts

[77] *See* Upjohn Co. v. United States, 499 U.S. 383, 294 (1981); Cicel (Bejing) Sci. & Tech. Co., Ltd. v. Misonix, Inc., 331 F.R.D. 218, 231 (E.D.N.Y. 2019); In re Kellogg Brown & Root, Inc., 756 F.3d 754, 758–59 (D.C. Cir. 2014) ("So long as obtaining or providing legal advice was one of the significant purposes of the internal investigation, the attorney privilege applies, even if there were also other purposes for the investigation and even if the investigation was mandated by regulation rather than simply an exercise of company discretion.").

[78] *See* United States v. Ruehle, 583 F.3d 600, 609 (9th Cir. 2009) (privilege did not apply to CFO's comments to attorneys where he understood that "the fruits of [law firm]'s searching inquiries would be disclosed to Ernst & Young . . . to convince the independent auditors of the integrity of Broadcom's financial statements to the public, or to take appropriate accounting measures to rectify any misleading reports").

merely because someone communicated that information to an attorney.[79] As a result, managing communications between counsel and the client's employees during an internal investigation requires a careful approach, as do issues related to notetaking, preparing a report, or even revealing the existence of an internal investigation.

3.5 Weighing the benefits of cooperation against the prospect of potential litigation.

3.5.1 Cooperation

Cooperating with a government investigation can have considerable benefits, particularly given the nature of criminal investigations and prosecutions of business entities. As business entities, health care providers can be criminally liable for the acts and omissions of their agents committed within the scope of the agents' duties on behalf of the provider.[80] Said differently, an employer can be guilty of its employees' crimes. As such, criminal charges can potentially be mitigated or avoided if would-be entity defendants act decisively to identify, tell the government about, and hold accountable the individuals responsible for wrongdoing.[81]

Under principals of federal prosecution, companies that cooperate with federal criminal investigations may experience reduced penalties, reduced charges, or even, potentially, no charges.[82] The Justice Manual (formerly known as the U.S. Attorneys' Manual) instructs federal prosecutors to consider the following factors in determining whether to seek charges against a corporate entity:

- The nature and seriousness of the offense.
- The pervasiveness of the wrongdoing and whether management was complicit.
- The corporation's history of similar misconduct, including prior criminal, civil, and regulatory enforcement actions against it.
- The corporation's willingness to cooperate (including with respect to its agents' wrongdoing).
- The adequacy and effectiveness of the corporation's compliance program both at the time of the offense and at the time of the charging decision.
- Whether the corporation timely and voluntarily disclosed wrongdoing.
- The corporation's remedial actions, including efforts to implement an adequate and effective compliance program, improve an existing one, discipline or terminate wrongdoers (including responsible management personnel), or pay restitution.
- Collateral consequences, such as disproportionate harm to shareholders, pension holders, employees, and those not proven personally culpable, as well as the impact on the public from a prosecution.
- The adequacy of civil or regulatory enforcement actions.
- The adequacy of prosecuting the responsible individuals.
- The interests of any victims.[83]

---

[79] *Upjohn*, 499 U.S. at 395.

[80] *See* Justice Manual 9-28.210(B) (describing the doctrine of *respondeat superior*).

[81] *See* Justice Manual 9-28.700 (cooperating with the government requires identifying, to the extent practicable, the individual employees "substantially involved in or responsible for the misconduct at issue, regardless of their position, status or seniority," and providing the DOJ with all relevant facts relating to the misconduct.).

[82] *See generally* Justice Manual 9-28.600, .700, .720.

[83] Justice Manual 9-28.300.

One of the most important factors is the role and conduct of management.[84] Effective cooperation with the government thus requires candor, honest introspection, and, potentially, difficult decisions. Similarly, effective cooperation may go hand in hand with a thorough internal investigation, because "[i]f a company seeking cooperation credit ***declines to learn of such facts*** or to provide the Department with complete factual information about the individuals substantially involved in or responsible for the misconduct, its cooperation will not be considered a mitigating factor."[85]

As this discussion suggests, voluntarily disclosing potential violations may—if done correctly—help make the case that prosecuting a health care provider is not necessary or appropriate. Depending on the situation, the government's priority in a given case may be not to punish or deter, but rather to establish compliance standards or bring money back into government health programs. If that is the case, good-faith and voluntary disclosure can go a long way. This is true in both the civil and criminal contexts.

Health care providers that choose to self-report must do so in the proper manner and through appropriate channels. First, the disclosure must be truly voluntary and must involve something worthy of disclosure; DOJ will not applaud a provider for disclosing something that the law requires to be disclosed or that does not involve a potential compliance violation.[86]

Second, voluntary disclosure is most effective if made quickly after the health care provider identifies the conduct at issue. For example, health care providers cannot invoke False Claims Act provisions authorizing reduced damages for self-reporting defendants unless the provider discloses the violation to DOJ within 30 days of discovering it.[87]

Third, the health care provider should disclose the potential violation thoroughly and in good faith. Selectively disclosing or attempting to conceal information can backfire, resulting in damaged credibility, a more confrontational investigation, and increased likelihood of criminal charges.[88]

Fourth, health care providers must utilize the correct self-reporting procedures. OIG oversees a Provider Self-Disclosure Protocol (SDP), under which providers can submit disclosures online through the OIG website.[89] For violations of the Stark Law (which OIG's SDP does not cover),

---

[84] Justice Manual 9-28.500(B).

[85] Justice Manual 9-28.700(A) (emphasis added); *see also* Justice Manual 9-28.720 (explaining that a corporation need not waive attorney-client privilege or work product protection to be eligible for cooperation credit, so long as the corporation discloses the relevant facts concerning the misconduct, i.e., how and when it occurred, who promoted or authorized it, or who committed it).

[86] *See, e.g.*, *OIG's Provider Self-Disclosure Protocol (Updated)*, U.S. DEP'T OF HEALTH & HUM. SERVS., OFF. OF INSPECTOR GEN., at 3 (Apr. 17, 2013), https://oig.hhs.gov/compliance/self-disclosure-info/files/Provider-Self-Disclosure-Protocol.pdf (conduct is not eligible for OIG's Provider Self Disclosure Protocol unless the disclosing party reasonably believes that the conduct "potentially violate[s] federal criminal, civil, or administrative law" for which OIG's civil monetary penalty authorities are authorized).

[87] *See* 31 U.S.C. § 3729(a)(2).

[88] Justice Manual 9-28.730 ("Another factor to be weighed by the prosecutor is whether the corporation has engaged in conduct intended to impede the investigation. Examples of such conduct could include: inappropriate directions to employees or their counsel, such as directions not to be truthful or to conceal relevant facts; making representations or submissions that contain misleading assertions or material omissions; and incomplete or delayed production of records.").

[89] *Provider Self Disclosure Protocol*, U.S. DEP'T OF HEALTH & HUM. SERVS., OFF. OF INSPECTOR GEN., https://oig.hhs.gov/compliance/self-disclosure-info/protocol.asp.

CMS administers a Voluntary Self-Referral Disclosure Protocol.[90] Also, in the civil False Claims Act context, DOJ has implemented a self-reporting program under which health care providers can receive cooperation credit for voluntarily disclosing violations, cooperating with the government's investigation, and taking remedial actions in response to an False Claims Act violation.[91]

Voluntarily disclosing potential violations to the government is not without its risks. Providers should consult with counsel and consider carefully whether to utilize the government's self-disclosure procedures.

3.5.2 Resisting enforcement through litigation.

Rather than cooperate, a health care provider may decide to resist or challenge the government's requests for information. Although it is common to negotiate with the government about the scope or timing of a document production or interview, occasionally it will not be possible to reach an agreement. Depending on the type of request and the nature of the impasse, the party that received a subpoena or CID may file an action to quash or narrow, or the government will initiate an action to enforce. In most circumstances, objecting providers should move to quash to avoid possible sanctions for failure to timely respond. The time to quash or modify a subpoena or CID is typically limited. For instance, a party receiving a CID related to a federal false claims investigation must file a petition to modify or set aside the CID either before the CID's return date or within 20 days, whichever is sooner, unless the government investigator allows for additional time.[92] CIDs issued by the Washington State Attorney General's Office require the receiving party to file objections with the superior court within the same time frame.[93] While it may be possible through litigation to limit or narrow some aspects of the government's request for information, a health care provider who chooses this option faces significant uncertainty about the odds of persuading a court to wholly invalidate a properly drafted subpoena or a CID.

For example, the scope of discovery under the Federal Rules of Civil Procedure governs the extent to which a CID will be enforced.[94] As such, arguing that a CID is overbroad, vague, unduly burdensome, or seeks irrelevant material[95] may succeed in limiting its scope, but it likely will not totally block enforcement in significant part unless the CID is fundamentally deficient or seeks wholly irrelevant information.

Similarly, the Fourth Amendment applies much less stringent standards to subpoenas than searches and seizures,[96] which require warrants based on probable cause (or an exception to the warrant requirement). Under the Fourth Amendment, subpoenas are generally valid if they are issued with

---

[90] *Self-Referral Disclosure Protocol*, CTRS. FOR MEDICARE & MEDICAID SERVS., https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/Self_Referral_Disclosure_Protocol.

[91] Justice Manual 4-4.112.

[92] 31 U.S.C. § 3733(j).

[93] RCW 19.86.110.

[94] *See* 31 U.S.C. § 3733(b)(1)(B); RCW 74.66.120(3)(b) (same with respect to Washington CIDs and the superior court civil rules); 31 U.S.C. § 3733(j)(6) (Federal Rules of Civil Procedure govern enforcement actions); RCW 74.66.120(30).

[95] *See* Fed. R. Civ. P. 26(b)(1) (scope of civil discovery), (b)(2) (orders limiting the frequency or extent of discovery), (c) (orders protecting parties from annoyance, embarrassment, oppression, or undue burden or expense).

[96] *See, e.g.*, United States v. Dionisio, 410 U.S. 1, 9 (1973) ("It is clear that a subpoena to appear before a grand jury is not a 'seizure' in the Fourth Amendment sense . . . .").

lawful authority, seek documents relevant to the government's inquiry, and are not so sweeping or indefinite that complying would be unreasonable.[97] A challenge may be worth considering, however, if there is a flaw in how a subpoena was authorized, issued, or served or if enforcement would impinge on a constitutional or common law privilege, such as the Fifth Amendment privilege against self-incrimination or the attorney-client privilege.

Challenging a search warrant is a different matter. Warrant applications are *ex parte* proceedings, so it is generally possible to challenge a warrant only after the search or seizure has happened.[98] Challenges after execution of a search warrant center not on whether the government can obtain or review the information, but rather on whether the government can use that information in the prosecution.[99] Answering that question will depend on the requirements for a valid warrant and a search under Fourth Amendment jurisprudence (e.g., defective warrant application, search outside the warrant's scope). This underscores the importance of having counsel present during a search, when possible, as counsel can lodge objections and document any improper conduct by the government, such as searching or seizing items not identified in the search warrant.

4 Readiness for government investigative inquiries.

Establishing sound policies and procedures for both legal compliance and responding to government inquiries is vital not just to successfully navigating an investigation, but also to reducing the likelihood of issues or misconduct arising that could prompt government scrutiny in the first place.

4.1 Providers should enact policies and procedures for responding to information requests from the government.

Health care providers should establish a written policy for receiving, evaluating, and responding to government investigative inquiries.

For instance, with respect to written requests for information, such as CIDs and subpoenas, the policy should designate a coordinating person, usually within the health care provider's in-house legal or compliance department, to whom all subpoenas, CIDs, and the like should be sent. This will allow the health care provider to identify and retain legal counsel to address the request and will avoid the risk that the recipient of the inquiry might fail to comply with the response deadline.

A written policy should also state how employees should respond if government agents execute a search warrant, which often happens unexpectedly and can significantly interrupt business operations. The policy should designate a trained search warrant response team, including in-house counsel and compliance personnel, with a member of the team located at each company site. Upon discovering that the government intends to execute a search warrant, the policy should specify a person to be contacted immediately to ensure a prompt response. The policy should also seek to have counsel present who can obtain a copy of the warrant, the names and contact information of the agents or officers executing the warrant, and a list of everything taken. Having counsel present can also help ensure that the government does not search for or seize an item that is outside the scope of the search warrant. Where that is not possible, the search warrant response plan should involve counsel visiting the site of the search to

[97] See v. City of Seattle, 387 U.S. 541, 544 (1967); United States v. Morton Salt Co., 338 U.S. 632, 652–53 (1950); Okla. Press Pub. Co. v. Walling, 327 U.S. 186, 209 (1946).

[98] As mentioned above, it is critical that employees not obstruct the government's search because obstructing may result in separate criminal charges. *See* Sec. 2.3.6.

[99] *See also* 42 U.S.C. § 1983 (authorizing private lawsuits against government actors for violations of civil liberties).

determine what the government took, how the search was executed, and the nature of any communication between agents and employees at the site.

In addition, a policy addressing search warrants should provide for contingencies to ensure that documents critical to business operations are not lost. Health care providers should segregate privileged documents from other types of records and maintain backups of mission-critical documents and records. Original documents seized by agents could be inaccessible for months or longer, making redundancies an important part of any policy addressing search warrant compliance and responses.

The policy should also address impromptu requests for information outside the search warrant context, such as what to do if an investigator appears at a company facility or an employee's home and requests information. On this subject, the procedures described above in Section 3.2 for appropriately communicating with employees about the existence of an investigation and their rights and obligations serve as solid starting point for crafting an effective response policy.

As this review of select policy provisions indicates, an effective policy for addressing government investigations must work alongside a comprehensive document retention policy. In addition to ensuring the availability of records needed for ongoing operations and for compliance purposes, a comprehensive document retention policy must also contain provisions that satisfy health care providers' legal obligations with respect to patient access and privacy. These issues are addressed in detail elsewhere in the Washington Health Law Manual.[100]

4.2 Compliance programs and organizational culture.

Companies establish compliance programs to police themselves, detect and prevent misconduct, and ensure that company operations comply with the law.[101]

A properly structured compliance program should provide training for employees on the applicable legal and regulatory requirements for, among other things, billing, reimbursement, and health care services in general. Employees should also receive instruction on how to report compliance issues and on the protections that safeguard people who make such reports. The program should also provide for periodic audits to ensure its efficacy. The audits should happen at a level sufficient to ensure that they are independent and accurate, and they should utilize a reporting system that will give management and directors prompt, accurate information from which they can reach an informed decision about their organization's legal compliance.[102]

As part of the framework it uses to determine whether to pursue criminal charges against a corporation, DOJ evaluates the adequacy and effectiveness of the corporation's compliance program.[103] The mere existence of a compliance program, however, is insufficient to justify not charging a corporation for its employees' or agents' crimes.[104] Companies should not enact mere "paper policies" to which they only pay lip service, but rather compliance programs that are "adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees" and that management actively

---

[100] Laird A. Pisto, *Maintenance of Business Records*, *in* WASH. HEALTH L. MANUAL, Ch. 28 (3d ed.).

[101] *See* Justice Manual 9-28.800.

[102] *Id.* (citing In re Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 968–70 (Del. Ch. 1996)).

[103] Justice Manual 9-28.300.

[104] Justice Manual 9-28.800.

enforces.[105] "The fundamental questions any prosecutor should ask are: Is the corporation's compliance program well-designed? Is the program being applied earnestly and in good faith? Does the . . . program work?"[106]

As these quotations from the Justice Manual suggest, the adequacy of a health care provider's compliance program depends in part on whether the broader company culture prioritizes compliance and integrity as norms for employees to follow.[107] To quote Preet Bharara, a former U.S. Attorney for the Southern District of New York, "[Y]ou have to say the corny stuff: 'We don't lie. We don't cheat. We don't steal.' Whatever those principles are, you have to say them all the time. That's important."[108]

[105] *Id.*

[106] *Id.*

[107] *See, e.g.*, Justice Manual 9-28.010 (among the foundational principals of corporate prosecution are "discouraging business practices that would permit or promote unlawful conduct at the expense of the public interest"); 9-28.200 (explaining how indicting a corporation for wrongdoing may serve as a "positive change of corporate culture"); 9-28.500 (in assessing whether to pursue criminal charges against a company for the misconduct of an employee, one of the most important factors is the role of management in shaping corporate culture); 9-28.600 (in assessing the corporation's past history, "[a] history of similar misconduct may be probative of a corporate culture that encouraged or at least condoned such misdeeds, regardless of any compliance programs").

[108] Jaclyn Jaeger *'You Have to Say the Corny Stuff': A Compliance Conversation with Preet Bharara*, COMPLIANCE WK. (May 21, 2019 10:24 PM), https://www.complianceweek.com/you-have-to-say-the-corny-stuff-a-compliance-conversation-with-preet-bharara-/27129.article.