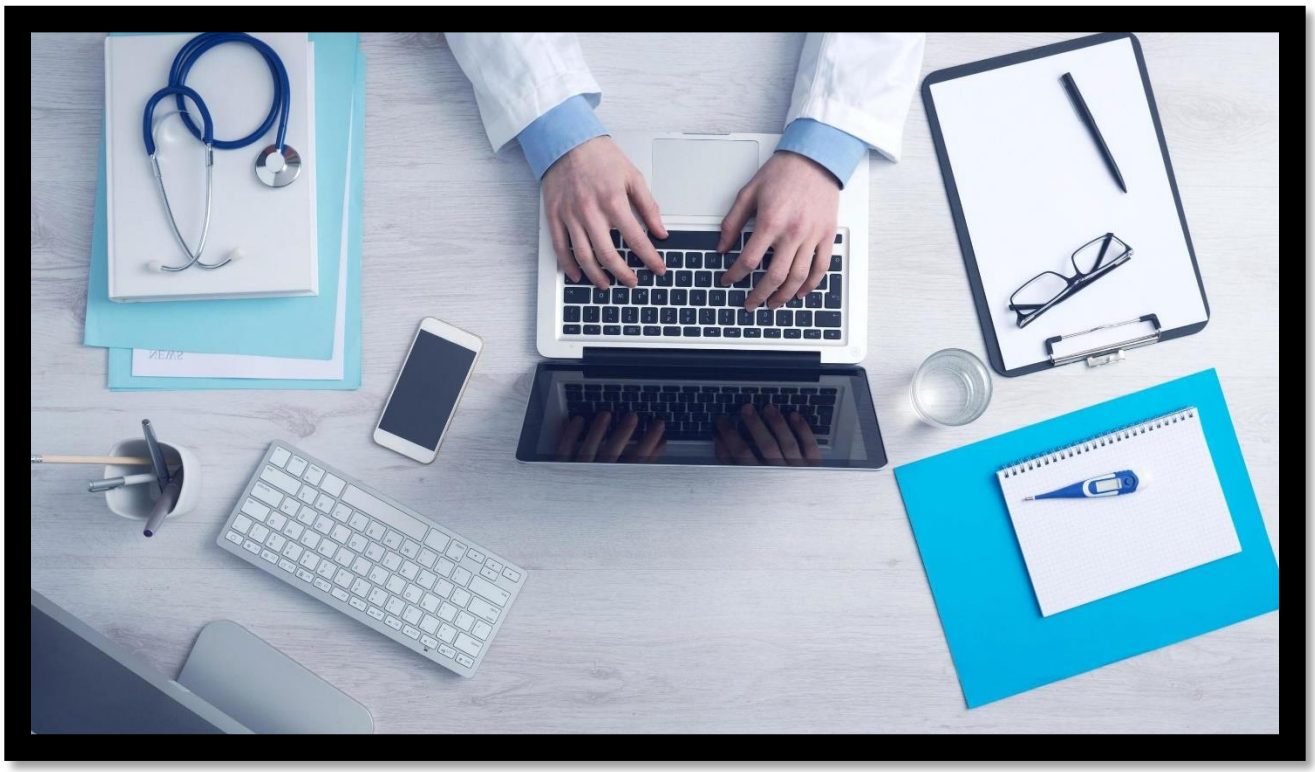


GUIDE

TO RESPONDING TO GOVERNMENT

INVESTIGATIONS

Ronald W. Chapman II, J.D., L.L.M.
M.K. Wickens, J.D., CFE, CHC

COPYRIGHT NOTICE AND DISCLAIMER

This publication is intended to serve as a preliminary research tool for attorneys. It is not intended to be used as the sole basis for making critical business or legal decisions. This document does not constitute, and should not be relied upon, as legal advice.

TABLE OF CONTENTS

ABOUT THE AUTHORS

Ronald W. Chapman II, Esq., L.L.M.

Ron is the managing shareholder of Chapman Law Group's Michigan Office and represents clients nationally in the areas of health care fraud and abuse, health care compliance, federal investigations, DEA registration matters, and physician licensing defense.

Ron has been published in national publications in the areas of defending physician overprescribing, health care compliance, and federal criminal defense. His work on litigation health care fraud allegations was recently published in the National Association of Criminal Defense Lawyers publication, *The Champion.*

Ron has also been invited to speak nationally on the area of health care compliance by the American Conference Institute, the International Conference on Opioids at Harvard Medical School, the Florida board of pharmacy, and he regularly lectures for the Michigan State Medical Society.

Mary Wickens, J.D., CFE, CHC

Mary has over thirty-five years of experience in health insurance, managed care, health care compliance, and litigation. Her experience includes advising and counseling health care providers, insurers, CMS, government contractors, and others in compliance, ethics, fraud and abuse, Medicare, Medicaid and Federal Employees Plan, managed care, and other matters.

Mary served as Assistant General Counsel and Compliance Officer for BCBSM and Blue Care Network for more than ten years, where she was managed responses to DOJ, HHS-OIG, OPM-OIG, and other government investigations and audits.

Mary has also served as the chief legal officer and subject matter expert for a CMS Medicare program safeguard contractor and consulted to CMS on its Medicare Part D fraud, waste, and abuse policies and manuals. She assists health care providers in developing and implementing effective compliance programs; in responding to audits and investigations; and, in conducting internal investigations.

Mary provides consulting and testifying litigation support, including skilled expert case review, written reports, and testimony in federal False Claims Act cases, arbitrations, and provider-payer disputes. She has experience as an effective testifying expert in FCA cases, managed care disputes, and commercial arbitrations.

Mary is listed on experts.com and S.E.A.K., her website is www.wickens-law.com.

GUIDE TO RESPONDING TO GOVERNMENT INVESTIGATIONS

I. Introduction

There is probably no industry regulated more than the health care industry. Numerous government agencies and private organizations watch over every decision a health care entity makes. Health care entities face investigations by numerous private and government entities. The Department of Justice is aided by the Drug Enforcement Administration, Centers for Medicare Services, the Office of Inspector General, the HEAT Task Force, State Medicare Fraud Control Units, and Zone Program Integrity Coordinators in its efforts to counteract health care fraud, waste, and abuse. These entities often work together during parallel investigations of health care entities in order to enforce a broad range of civil, administrative, and criminal regulations.

This paper provides an overview of the types of health care regulatory investigations as well as basic strategies for effectively representing a broad range of health care clients when dealing with government investigations.[1] Practitioners should be aware that health care investigations are a highly specialized area of practice, and ABA Model Rule 1.1 requires an attorney to possess competence in the area of law he or she practices. Before aiding a client in a health care investigation, counsel should be sure that it possesses competence or a willingness to employ experts, investigators, and co-counsel who are experienced in the area of investigation. Not only are the stakes high, civil fines, recoupments, and forfeitures can be in the millions, and Federal Sentencing Guidelines are not friendly to those convicted of committing fraud.

The Office of Inspector General (OIG) encourages, and, in some cases, federal regulations demand, that health care entities have an effective compliance program in place that is reasonably likely to detect fraudulent conduct.[2] Much of the discussion in this paper deals with how to react to notice of a government investigation; however, a compliance plan may alleviate the need for such a reactionary approach. A robust compliance program that is properly developed,

implemented, and regularly improved will help detect compliance issues before they become the subject of investigations. Quickly convening an internal investigation to discover the scope of the issue and practicing proper reporting of overpayments will, in most cases, extinguish the "knowledge" element of health care fraud statutes and ensure that an administrative or civil matter remains in the administrative or civil realm. Attorneys will always have clients who are unaware of their compliance responsibilities or who have failed to detect and extinguish fraudulent conduct, and it is these clients that are at the greatest risk of increased government attention.

Before exploring the process for assisting health care clients facing government investigations, it is important to explore the relevant federal and state entities and their roles and responsibilities.

II. Government Agencies

A. The Department of Health and Human Services and its Associated Entities

The Department of Health and Human Services (HHS) is a cabinet-level department of the federal government. HHS's stated mission is to protect the health of "all Americans" and provide essential human services. HHS is composed of agencies and offices serving its regulatory and operational functions, including the Office of Civil Rights, the Office of the Inspector General, Center for Medicare and Medicaid Services, the Departmental Appeals Board (DAB), Substance Abuse and Mental Health Services (SAMSA), and the Food and Drug Administration (FDA).[3]

The Office of the Inspector General (OIG) is a regulatory office of HHS. The OIG is responsible for conducting criminal, civil, and administrative investigations into fraud and misconduct related to federal health care programs. In addition to investigative powers, the OIG has the authority to exclude providers from participation in a federal health care program.[4] The OIG also has the authority to impose civil penalties on health care providers.[5]

The Office of Civil Rights (OCR) is the regulatory office of HHS which enforces compliance with civil rights laws, including, but not limited to, constitutional civil rights, HIPAA, and the Patient Safety Act. The goal of the OCR is to aid in protection of fundamental rights of nondiscrimination, religious freedom, and privacy of health information. While the OCR has investigative authority over all recipients of financial assistance from HHS, its primary involvement with providers is its authority to enforce the privacy components of the Health Insurance and Accountability Act of 1996 (HIPAA) and the Health Information Technology and Reinvestment Act of 2009 (HITECH). The OCR enforces HIPAA violations pursuant to the HIPAA enforcement rule, which is codified at 45 CFR Part 160.

Centers for Medicare and Medicaid Services (CMS) is an operational agency of HHS consisting of four consortia (Medicare, Medicaid, Financial Management, and Quality Improvement), which collectively serve roles as a representative body for Medicare and Medicaid. CMS primarily administers Medicare, Medicaid, and the Children's Health Insurance Program (CHIG). On behalf of HHS, CMS has the authority to investigate complaints and audit providers for compliance. CMS also has other responsibilities, including the administrative simplifications standards from HIPAA, quality standards in long-term care facilities, and clinical laboratory quality standards under the Clinical Laboratory Improvement Amendments (CLIA).

B. Department of Justice Strike Force

The Department of Justice (DOJ) is comprised of approximately 40 units that handle a wide range of criminal justice, national security, and law enforcement responsibilities. In May 2009, the DOJ and HHS announced the creation of a new unit, the Health Care Fraud Prevention and Enforcement Action Team (HEAT).[6] The sole duty of the team is to enforce federal statutes related to health care fraud, waste, and abuse and to augment existing health care fraud strike force. Each HEAT team is assigned an HHS-OIG agent and FBI agent and is also partnered with State

Medicaid Fraud Control Units and local law enforcement. Currently, the DOJ has a strike force presence in Los Angeles, Texas, Baton Rouge, Detroit, Chicago, New York, Miami, and Tampa.[7] As of January 2018, the strike force claims responsibility for 1,938 criminal actions, 2,498 indictments, and recoupment of $3,005,949,223 in Medicare/Medicaid spending.[8]

C. Drug Enforcement Administration

The Drug Enforcement Administration (DEA) is responsible for enforcing controlled substances laws through prosecution of criminal and civil violations. The primary authority for its investigatory function is found in the Controlled Substances Act of 1970 (CSA).[9] While the DEA investigates controlled substances violations pertaining to all drugs, illicit or otherwise, the DEA Office of Diversion control is tasked with monitoring the manufacture, sale, and prescription of controlled substances. In order to carry out its administrative and regulatory function, the DEA frequently conducts audits of prescribers and pharmacies to determine compliance. These audits are typically triggered through an investigative tip from a pharmacy or patient, deviations in prescriber data such as MAPS data, or at random. An investigation for compliance with CSA begins upon receipt of DEA Form 82 (Notice of Inspection of Controlled Premises) or an administrative inspection warrant. However, if the DEA is engaged in a criminal investigation, a warrant for search and seizure of provider's practice is required. If the DEA finds noncompliance with the CSA, violations are either handled administratively through the use of a memorandum of understanding or order to show cause or are reported to the DOJ for criminal enforcement of the imposition of civil monetary penalties.

D. State Agencies

In addition to federal agencies, there are a number of state agencies responsible for investigating allegations related to federal health care programs. The Michigan Department of Health and Human Services (MDHHS) is charged with a broad array of functions and is similar to

the U.S. Department of Health and Human Services (HHS). MDHHS also works with HHS and the OIG to investigate suspected federal health program fraud. MDHHS has a special investigation unit that investigates criminal and civil complaints of fraud, waste, and abuse in the programs administered by the department.[10]

In addition, the Michigan Department of Licensing and Regulatory Affairs, Bureau of Professional Licensing (BPL) is charged with investigating health professionals suspected of violating the Michigan Public Health Code.[11] After an investigation is completed, the Michigan Attorney General Assigns an Assistant Attorney General to represent the BPL during proceedings before an administrative law judge. In addition to its regulatory function, the Michigan Attorney General's office also contains a Health Care Fraud Division. The division is comprised of attorneys, investigators, auditors, and other support staff, and has jurisdiction to investigate and prosecute Medicaid provider fraud and seek civil recovery of fraudulently obtained Medicaid dollars.[12]

III. Laws Against Health Care Fraud and Criminal and Civil Penalties: A Brief Overview

Various federal and state laws set out the possible statutory violations and penalties that can result from health care fraud investigations. Federal laws set out a vast array of criminal, civil, and administrative penalties and sanctions. Michigan false claims and insurance fraud laws contain their own criminal and civil penalties. The following is a brief overview of the major laws and their penalties.

A. Select Federal Laws and Penalties

The Criminal Health Care Fraud Statute[13] (18 USC 1347) makes it a crime to knowingly and willfully defraud any health care benefit program or to use false statements to obtain funds from a health care benefit program. Penalties include prison terms of up to 10 years and 20 years to life if the fraud results in serious bodily injury or death. Fines of up to $250,000

for individuals and $500,000 for organizations may be imposed,[14] together with court ordered forfeiture of property derived from the offense.[15] This law applies to both public and private health plans.

The Criminal False Claims Act (18 USC 287) imposes criminal liability when a defendant made or presented a false claim, knew that the claim was false, and did so with the specific intent to violate the law or with a consciousness of wrongdoing.[16] Violations can result in up to five years in prison and criminal fines of up to $250,000 per person and $500,000 per organization.[17]

The Civil False Claims Act (FCA) (31 USC 3729 – 33) prohibits anyone from "knowingly" presenting a false or fraudulent claim to the federal government. Civil penalties range from $10,957 to $21,916 per claim,[18] plus three times the amount of damages, and reimbursement of attorney fees and costs. Known as the "Lincoln Law" because it dates back to Civil War era fraud concerns, it applies to any claim to the federal government, not just health care. Several recent FCA settlements with pharmaceutical companies were over one billion dollars each. The DOJ reports 19.3 billion dollars in health care FCA judgments and settlements between 2009 and 2016.[19] The vast majority of these cases are settlements.

The Anti-Kickback Statute (AKS) (42 USC 1320a-7a) prohibits the knowing and willful, offer, solicitation, payment, or receipt of any remuneration, to induce or in return for referring an individual for health care for which payment may be made under a federal health care program.[20] Criminal penalties include fines of up to $25,000 and five years in prison. Violations of the AKS can also incur Civil Monetary Penalties (CMPs) of up to $50,000 for each violation plus three times the amount of the remuneration.[21]

Civil Monetary Penalties Law (CMP) (42 USC 1320a-7a)[22] authorizes HHS-OIG to impose civil penalties for violations of the FCA, the AKS, and other violations. Penalties under 1128A of the Social Security Act for violations of the AKS range from $10,000 to $50,000 per violation. There are, in fact, a vast array of CMPs that HHS-OIG and other agencies, including CMS and the FDA, can impose on Medicare Part C and D plans, health care providers, and others. Violations of HIPAA and HITECH[23] are investigated by the HHS Office of Civil Rights, and CMS investigates violations of the Stark Self-referral law and each has the authority to impose CMPs for violations. A comprehensive list of the CMPs, with the inflation adjusted amount, regulatory authority, and responsible agency is detailed and updated annually at 45 CFR 102.3. A current list of the CMP authorities is published by HHS-OIG on their website.[24]

Exclusion Provisions of the Social Security Act (42 USC 1320a-7a) mandates HHS-OIG and CMS to exclude from participation in Medicare, Medicaid, and other state health programs in certain instances, and permits exclusion in others. Exclusion is mandated where the individual or entity is convicted of criminal health care, neglect or abuse of patients, or felony unlawful distribution of controlled substance. The general exclusion period is five years.[25] A detailed list of the exclusion authorities and whether exclusion is mandatory, is available at the HHS-OIG website. [26]

Other laws often used by federal prosecutors in health care fraud cases include: False Statements,[27] Mail and Wire Fraud,[28] RICO violations,[29] Fraud Injunction Asset Freezes,[30] and Money Laundering Statutes.[31]

B. Select Michigan Laws and Penalties

The federal government strongly encourages each state to have its own False Claims Act (FCA) as a means of preventing health care fraud at the state level, especially in Medicaid. States that have a qualifying FCA receive financial incentives under section 1909 of the Social Security

Act, including increased Medicaid payments.[32] There are two primary Michigan laws against health care fraud.

The Michigan Health Care False Claims Act (MCL 752.1001 *et seq*) makes it a felony to knowingly submit a false or deceptive claim to a health care corporation (i.e., BCBSM) or health insurer for payment or benefits. It also contains an anti-kickback provision that makes it a felony to solicit, offer, pay, or receive a kickback or bribe in connection with any payment from a health care corporation or insurer. Penalties for violation of these provisions are up to four years in prison and a fine of up to $50,000, or both. A conviction for conspiracy to defraud a health insurer carries a possible prison term of 10 years. In the case of second offenses, fines and imprisonment can be doubled.

The Michigan Medicaid False Claims Act (MCL 400.601 *et seq*) likewise prohibits the knowing submission of any false or deceptive claim to Medicaid. It also makes it a crime to submit claims for medically unnecessary services and includes a reverse false claims provision. It contains an anti-kickback provision and includes criminal penalties for making false statements about the condition of a health care facility. Penalties range from four to 10 years in prison and fines of $30,000 to $50,000 or both. The Michigan Medicaid FCA includes civil penalties and *qui tam* provisions similar to the federal False Claims Act that can result in private *qui tam* recoveries on behalf of the state.

IV. Identifying the Type of Investigation

An important first step in every case is to identify the type of investigation and possible exposure to the client. Sometimes this is clear – for example, receipt of a grand jury subpoena clearly indicates a criminal matter, but many times first contacts are more nuanced. Obviously, the most serious situation for a client is criminal exposure which can result in frozen assets, loss of licenses, steep fines, and imprisonment. In most cases, a criminal investigation is underway long

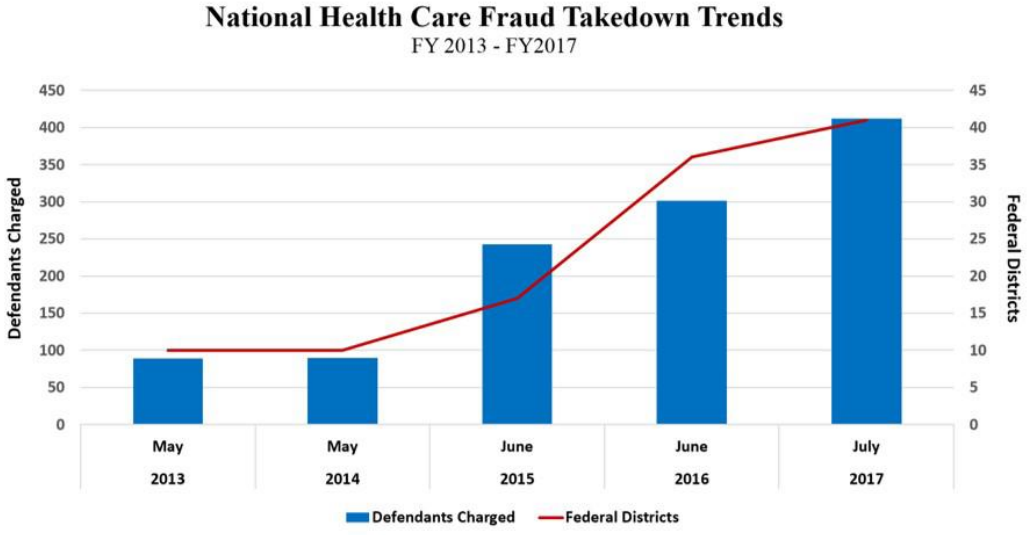
before the target or subject is even aware of the investigation. Even administrative cases often begin before the client is aware that their claims and other data is being mined for possible fraud or non-compliance.

Identifying the type of investigation and advising the client about the risk and possible penalties is both the first step in responding to any investigation and an ongoing task. It is important to remain vigilant and flexible as the matter progresses. What begins as an administrative or civil matter, may progress to a criminal investigation over time. As the investigation progresses, counsel can provide valuable knowledge and guidance by interacting with the government to learn more about the investigation, by cooperating with auditors and investigators, by conducting parallel or "shadow" internal investigations, and most importantly, by constantly understanding and applying new facts and information to their legal analysis, strategy, and client advice.

A. Criminal

Most audits and inquiries by the government are not criminal in nature. However, the consequences of a criminal fraud investigation can be catastrophic to the client. The majority (71%) of those convicted of health care fraud are sentenced to prison and the average sentence is just under three years.[33] Pre-trial asset freezes can devastate an organization or individual. Fines from overlapping statutes can be in the millions of dollars, and the legal fees and costs associated with defending such cases are daunting. Felony convictions for health care fraud, patient abuse, or related to controlled substances will result in mandatory exclusion from Medicare and Medicaid and other health care programs.[34] Additionally, virtually all private payors will refuse to pay or employ any excluded provider. As a result, every health care organization and their lawyers should have a plan to address possible allegations of criminal wrongdoing as a proactive measure, and that plan must include swift action and inclusion of counsel at the earliest possible stage.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established the Health Care Fraud and Abuse Control Program (HCFAC) under the joint direction of the Department of Justice (DOJ) and the Department of Health and Human Services, Office of Inspector General (HHS-OIG).[35] In FY 2017, the DOJ opened 967 new criminal fraud investigations, and prosecutors filed criminal charges in 439 cases involving 720 defendants.[36] In a recent joint report to Congress, the DOJ and HHS-OIG report a significant upward trend in the number of defendants charged across an increasing number of federal jurisdictions. [37]



The government takes a highly collaborative approach to health care fraud investigations and prosecutions. Under the HCFAC program, the DOJ and HHS-OIG operate the joint Health Care Fraud Prevention and Enforcement Action Team (HEAT), including the Medicare Fraud Strike Force (MFSF) and Medicaid Fraud Control Units (MFCUs). The DOJ, including United States Attorney Offices (USAOs), the FBI, and OIG-HHS, conduct criminal health care fraud investigations at the federal level, while the Attorney General in each state is generally responsible for prosecutions of health care fraud at the state level. Often criminal investigations are conducted jointly by various government agencies, such as the DOJ's USAOs, FBI, Office of Inspector

General (HHS-OIG), Drug Enforcement Agency (DEA), and others. Private or commercial insurance fraud units (Special Investigation Units or SIUs) often cooperate with law enforcement. It is important to remember that defrauding a private or commercial health insurer can also bring about federal and state criminal penalties. Undercover operations are often conducted by the FBI in conjunction with state law enforcement and other agencies.

Often, the first indication that a criminal investigation is underway is contact by the FBI or other law enforcement agent with a current or former employee. In rare cases, initial contact may be in the form of a search warrant being executed by the FBI or other law enforcement. A search warrant indicates that at least one judge, usually a magistrate, believes that there is probable cause that a crime was committed and that evidence of the crime is located in the place to be searched.[38] The government usually uses search warrants where there is no real health care being provided, but rather, a clear criminal enterprise is underway.

An Authorized Investigative Demand (AID)[39] is another indication of a criminal health care fraud investigation. HIPAA empowered the DOJ to issue AIDs that are enforceable in federal court and without the constraints of grand jury subpoenas. While AIDs are authorized for criminal purposes, the data and records obtained can, and increasingly are, used in civil false claims cases. In addition, HHS-OIG has authority to subpoena documents and witnesses in both criminal and civil investigations.[40] An OIG subpoena may indicate that a criminal or civil investigation is underway.

It is important to distinguish AIDs from OIG subpoenas, the US Attorney's Manual describes AIDs and subpoenas as follows: "Investigative demands differ from inspector general subpoenas in that the scope of the latter are limited to the statutory authority of the specific

inspector general and civil investigations, whereas investigative demands can be directed more broadly to various public and private victims and must involve criminal investigations."[41]

A criminal probe is also indicated when a grand jury subpoena is issued or the client is contacted by an Assistant United States Attorney (AUSA) to appear voluntarily. The United States Attorney's Manual encourages the use of voluntary appearances before a grand jury and use of notification letters where appropriate.[42] An important factor is whether the AUSA involved is in the criminal or civil division of the United States Attorney's Office (USAO), keeping in mind that sometimes the two divisions work together on a particular case. If possible, it is important for counsel to determine whether the client is a target, a subject, or a witness of the investigation. As discussed below, counsel handling criminal health care fraud matters should, of course, have an effective professional relationship with the local USAO for their district and, in particular, with the health care fraud section in that district.

B. Civil False Claims

With its steep and compound penalties, the civil False Claims Act (FCA) is the preferred vehicle for federal officials to investigate and prosecute health care fraud matters. Notice of a civil false claims matter could come in a number of ways.

The receipt of a Civil Investigative Demand[43] (CID) clearly indicates a civil false claims investigation. The FCA authorizes the DOJ to issue a CID to require production of documents, answer interrogatories, and compel testimony in civil FCA investigations. CIDs often contain extensive requests for documents as well as electronic material, they spell out the format for producing electronic records, and often contain extensive interrogatories. An OIG subpoena is another indication of a civil or criminal investigation.

In some cases, the OIG will simply send a letter indicating a concern and asking for a response by the organization or individual. This may indicate an inquiry for the predicate for an investigation, or simply a follow up to a tip.

Investigators have broad authority to access the records of any entity or individual who participates in Medicare, Medicaid, or other public health programs, and this authority extends to HHS and its agents, like CMS, HHS-OIG, and state Medicaid Fraud Control Units.[44] An audit by one of these agencies can be routine but should be approached with caution especially if immediate access is demanded. Whether the audit is routine or part of an investigation should be established with the auditors at the entrance conference.

Other indicators of a civil false claims investigation can come from the CMS integrity contractor for the client's region. As indicated above, CMS uses Zone Program Integrity Contractors (ZPICs) to analyze data, receive tips, and investigate possible fraud, waste, and abuse in Medicare programs. A document request from the ZPIC indicates that an investigation into false claims or other payment violations is underway. If the ZPIC finds evidence of possible fraud, it will refer its findings to law enforcement and continue to support the ongoing investigation.

Finally, serious or repeated audit findings by the Medicare Administrative Contractor (MAC), Recovery Audit Contractors (RACs), or other agencies may trigger a broader investigation by the ZPIC, CMS, or HHS-OIG. The MAC and all other CMS contractors have an obligation to report any possible fraud, waste, or abuse in the Medicare, Medicaid, or other health care programs. Any entity or individual who has serious or repeat audit findings should consider it an early warning of possible further investigation.

C. Civil Monetary Penalties

Civil Monetary Penalties (CMPs) are assessed by the government in a vast array of circumstances. In addition to HHS-OIG's authority to impose CMPs for false claims and other

improper payments, agencies such as CMS, FDA, and DEA have CMP authority. The latest list of available CMPs, their adjusted amounts, and regulatory authority is published by HHS-OIG on its website.[45] CMS has authority to impose CMPs on Medicare Part C and Part D plans and does so routinely to penalize regulatory non-compliance.[46] CMPs are often used to impose penalties that are the result of negotiations between the entity or individual being regulated and the government, and can serve as a means to accept sanctions without admission of wrongdoing or guilt and possible program exclusions.

In the health care fraud context, HHS-OIG imposes sanctions for violations of the False Claims Act or the AKS and other improper payments. HHS-OIG will generally first send a notice of intent to impose CMPs, and this often occurs after an audit or an investigation identifies improper payments that do not warrant criminal or civil law enforcement action. This gives the target of the CMPs and their counsel an opportunity to defend and negotiate the findings and penalties. Most often, the CMPs are the result of an audit or other review, or in response to complaints or tips sent in to CMS or HHS-OIG.

Regulations found at 42 CFR Part 1003 set out the process, notice requirements, appeal rights, and other requirements for CMPs. All CMPs must be in writing and provide notice of the basis of the CMP authority, the law or regulation being violated, and the right to appeal the penalty to an Administrative Law Judge. Typically, this comes in the form of a letter from the OIG or CMS after negotiations with the government. In most cases, the entity or individual will also need to adopt certain corrective actions, which may include entering into a Corporate Integrity Agreement. As with other civil penalties, repeated or serious audits or program reviews are often the first indication of impending CMPs or other sanctions.

D. *Qui Tam:* Whistleblower Cases

The False Claims Act (civil) contains a *qui tam* or whistleblower provision that significantly expands the scope of those who can "investigate" and report health care fraud.[47] The DOJ reports that it recovered a total of $3.7 billion under the FCA in 2017, and of that amount, health care fraud made up $2.4 billion.[48] It is important to note that the vast majority, $3.4 billion, of civil FCA recoveries were the result of *qui tam* or whistleblower cases brought under the FCA.[49]

The FCA's *qui tam* provisions authorize any private party (aka "relator"), with direct knowledge of the fraud, to bring an action on behalf of the federal government. The relator must be the first to identify and report the fraud to the government. Cases are brought in federal court under seal and served on the DOJ only. The defendant is not initially served. The government or the relator, or both, will continue to conduct an investigation into the alleged fraud while the case is under seal. The target or subject may receive CIDs, OIG subpoenas, or less formal requests for information that might indicate an unsealed *qui tam* investigation.

Often, the relator is a current or former employee of the target, or may be an outside auditor, IT or software vendor, or even a patient or a competitor. Many times, the relator has reported the fraudulent activities to management or the compliance department with no resolution and engaged *qui tam* counsel as a last resort. Therefore, the combination of government subpoenas or other inquiries coupled with unresolved compliance complaints may indicate a potential, but still sealed, *qui tam* action.

The government may choose to intervene and prosecute the *qui tam* case, or it may decline to intervene and the relator will go forward on the government's behalf. If the government elects not to intervene, it does not mean that it does not have confidence in the case; it often means that the government will rely on the relator's counsel to litigate the case, and the decision can be as much about government resources as the merits of the case. *Qui tam* plaintiffs receive from 15%

to 25% of the recovery if the government intervenes, and 25% to 35%, plus attorney fees and expenses, if the government does not intervene. Once the complaint is unsealed, the target is served with the complaint to answer and defend. At that point, it is clear that there is a serious *qui tam* civil FCA investigation and prosecution underway.

V. Initial Contact

A. Responding to Federal Criminal Investigations

i. Grand Jury Investigations

For the purposes of federal criminal investigations, a "target" of a federal investigation is a person to whom the prosecutor 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."[50] A "subject" of an investigation is a person whose conduct is within the scope of the grand jury's investigation.[51] The first contact with the DOJ during a federal criminal investigation may be a grand jury target letter.

During federal investigations, it is more common for DOJ attorneys to contact a target prior to the issuance of a search warrant. Often, federal agents and attorneys do not wish to engage in the unnecessary risk associated with conducting searches of the target of an investigation and would rather obtain information using grand jury subpoenas and a grand jury investigation. A person or entity receiving a "target" letter can be sure that they are the target of a federal prosecution. Often, prosecutors will send a target letter to the person or entity under investigation, informing the recipient that it is the target of a federal investigation and encouraging the target to obtain counsel to facilitate testimony in front of a grand jury or respond to grand jury subpoenas for medical records or billing data. The target letter serves multiple purposes; for example, it puts the target on notice that destruction of documents may violate federal law, that the target has a right to obtain counsel, and that the target must answer any questions posed to the target truthfully.

A sample target letter can be found in the United States Attorney's Manual, and most districts send a similar letter.[52]

The origin of the target letter can be found in an amalgamation of federal case law finding that subpoenaing the target of a federal investigation has the appearance of unfairness because the target may not have access to counsel, or may not be able to properly raise claims of privilege or Fifth Amendment claims.[53] As a result, it is the policy of the DOJ to issue target letters prior to issuing a subpoena to a target of a federal investigation.[54] It is also DOJ policy to advise targets of their Fifth Amendment privilege against compulsory self-incrimination. While the Supreme Court has declined to decide whether a grand jury witness should be warned of his or her Fifth Amendment privilege, in *United States v. Mandujano*, the Supreme Court took notice of the fact that prosecutors customarily warn "targets" of their Fifth Amendment rights.[55] As a result of this custom, but lacking a constitutional imperative, DOJ policy requires prosecutors to warn targets of their rights prior to testifying before a grand jury.[56]

If a client receives a target letter, counsel can be certain that the federal government has begun an extensive investigation into the client's practice and is likely concluding that investigation and seeking an indictment. This should send a message to counsel that counsel is already many steps behind the government and the government has a significant informational advantage. Upon receipt of a target letter, counsel should speak with the assigned Assistant United States Attorney (AUSA) to find out as much information as possible about the potential charges, subject matter of the case, and the client's role in the investigation. Some AUSAs will be tight lipped about the investigation while others may be forthcoming with information in order to facilitate a pre-indictment resolution of the matter.

After learning as much about the case as possible, counsel must consult with the client and obtain approval to begin a parallel or "shadow" investigation into the perceived issue to determine the client's role and potential culpability.[57] This will also assist in the early preservation, gathering, and production of documents pursuant to the inevitable grand jury subpoena that the client is likely to receive.[58]

When a health care company is the subject of a grand jury investigation, the company's counsel should consider retaining independent counsel to represent employees of the company. It is imperative that employees receive representation during the grand jury investigation to protect their rights, make them more comfortable during the process, and protect potentially privileged information. While successive representation of the corporation and its employees is theoretically possible if no conflict exists, this is not advisable given that counsel will likely lack sufficient knowledge of the subject and scope of the investigation, as well as the actions of all employees, to make a worthwhile conflict determination.[59]

ii. Responding to Documentary Requests Generally

Regulatory and law enforcement authorities have a vast number of compulsory production tools at their disposal. In the administrative context, regulators may utilize administrative subpoenas or audits to gather patient records and other material of evidentiary value. The DOJ and state regulators using civil enforcement means may utilize civil subpoenas, requests for production of documents, and requests pursuant to Federal Rule of Civil Procedure 26 to obtain records. In addition, the DOJ may utilize Civil Investigative Demands (CID) pursuant to 31 USC 3733. When the target of any type of investigation receives a demand for compulsory documents, there are a few essential steps that must be undertaken by counsel or the investigation team regardless of the type of request, such as preservation, review, and production of relevant materials.

Prior to responding to the compulsory production request, counsel must first review the relevant request. This will give counsel vital information about the scope, target(s), subject matter, and focus of the investigation. In many cases, review of the document may suggest that the entity receiving the document is not the target of the investigation, but rather a subject or even a witness. For instance, a toxicology laboratory that receives a CID for its lab requisition forms for one particular provider is not likely to be an investigation into the laboratory, but an investigation of the provider instead. Alternatively, if the CID issued to the laboratory requests requisition forms, lab results, and the contract with the lab's medical director, the lab is likely one of the targets of the investigation.

Preservation of relevant material is the first step that must be taken by the target of any investigation. After reviewing the request, counsel will also understand what documents are sought and can prepare a plan for preserving, reviewing, and producing relevant material. Counsel should construe a government request in the broadest sense possible when reviewing the request to preserve documents. This must occur when the target first learns that it is the target of an investigation through notification of an audit, a target letter, or correspondence from a regulatory body. Preservation usually comes in the form of a litigation hold and effective policies and procedures that direct the organization how to respond to a litigation hold. Some circuits have expanded this duty to require preservation when a "government inquiry is reasonably anticipated, threatened, or pending."[60] This duty requires "reasonable" and "good-faith" actions to preserve potentially relevant information related to the anticipated litigation.[61] In order to properly preserve potentially relevant information, counsel should work with the target to identify all sources of information and any means by which data could be spoiled or destroyed, and properly communicate the need to preserve potentially relevant data for later review. Effective policies and

procedures regarding data retention and destruction will be valuable in achieving this goal by providing a uniform method of document preservation and destruction that will allow counsel to temporarily modify to prevent document spoliation.

After counsel has had an opportunity to submit a preservation request to employees and preserve relevant data, counsel must then begin the process of gathering and reviewing responsive data to determine if the data is *(1)* responsive to the request and *(2)* non-privileged. This process must begin by gathering all potentially responsive information regardless of privilege. A spreadsheet or database should be created so that counsel can track whether information has been reviewed and if an assessment has been made as to its responsiveness to the request and potential privilege. This will prove useful in creating a privilege log later. For example, the spreadsheet could contain the following headings:

FIGURE X-X

Title	Custodian	Date Reviewed	Responsive?	Privileged?	Date Produced

As each document is reviewed, counsel should make a notation on the spreadsheet and sufficiently describe the basis for non-production due to a claim of privilege or that the document is non-responsive to the request. For email correspondence, the log should also contain the sender, recipient, and any carbon copy (cc) information. Information regarding privilege should be sufficiently detailed in order to support future objections that the information is privileged.[62] The log must be updated as additional documents are reviewed and the log must clearly indicate the date of production to the government and any objections.

Privileges and Their Applicability

There are several types of privilege associated with government health care investigations,[63] such as *(1)* the attorney-client privilege, *(2)* the work product doctrine, and *(3)* the Fifth Amendment privilege.

The attorney-client privilege is an absolute protection to most confidential communications between clients and their lawyers. The privilege is codified in the Federal Rule of Civil Procedure 26(b)(1) and Rule 501 of the Federal Rules of Evidence, which holds that the privilege shall be governed by principles of common-law. In order for the privilege to apply, two of the following elements must be met: *(1)* the communication must be confidential; *(2)* the communication was made to an attorney; or *(3)* the communication was made in connection with rendering legal advice or assistance.[64]

The attorney-client privilege only applies to the content of the communication itself and not the fact that the communication occurred.[65] Courts are divided regarding the scope of the privilege, but the Sixth Circuit stands with the majority of courts in holding that the privilege does not automatically extend to mundane facts, such as the identity of the client, the general nature of services, and matters of public record.[66] The privilege is more likely to stick to substantive legal advice unless disclosure of other information would be tantamount to disclosure of confidential information.[67]

There are two principal ways in which the privilege can be waived, which are voluntary disclosure and the crime-fraud exception. Generally, the "attorney-client privilege is waived by voluntary disclosure of private communications by an individual or corporation to third parties. Voluntary disclosure in Michigan requires a knowing and intentional act, inadvertent disclosure does not waive a privilege".[68] A client may also waive the privilege by conduct which implies a

waiver of the privilege or consent to disclosure.[69] This waiver includes voluntarily disclosing privileged documents to the government in response to the compulsory process.

In addition, the attorney-client privilege may be waived by the "crime-fraud exception" which has been adopted by the federal courts as well as Michigan state courts.[70] The crime-fraud exception is rooted in the notion that attorney advice facilitating the commission of a future wrongdoing should not be shielded from disclosure.[71] In order to invoke the crime-fraud exception, the government bears the burden of establishing that *(1)* there is probable cause to believe that the client committed a crime, fraud, or breach of duty, and *(2)* that the attorney's assistance or advice was obtained in furtherance of the criminal or fraudulent activity.[72] However, the extent to which information is covered by the attorney-client privilege is likely to change due to recent events undertaken by the United States government to contract the scope of the privilege.

The Work Product Doctrine

The work product doctrine is set forth in Federal Rule of Civil Procedure 26(b)(3) and protects materials prepared in anticipation of litigation or trial, by or for the party to the litigation or his representative.[73] The doctrine also protects draft reports required by Rule 26(a)(2) of testifying experts and most communications between attorneys and experts.[74] Information sifted by counsel from a larger set of information is protected if the culling of information was pursuant to a deliberative process.[75] Courts generally hold that work product prepared to respond to a government investigation generally is enough to invoke the work product doctrine.[76] Counsel should clearly mark information that is work product when possible to avoid confusion over what information is protected and to avoid inadvertent disclosure.

The Fifth Amendment Privilege

The Fifth Amendment does not apply to corporations, but may be invoked by an individual whom the government seeks to compel to testify or provide documents that may be incriminating.[77] Moreover, "[a] custodian may not resist a subpoena for corporate records on Fifth Amendment grounds".[78] This prohibition even applies to sole proprietorships where the company only has one employee.[79] However, the Fifth Amendment does apply to individual defendants and, if potential criminal culpability is possible, employees should be advised of their Fifth Amendment rights and obtain separate counsel if their interests in protecting those rights are adverse to those of the corporation.

The Fifth Amendment provides two categories of protection: *(1)* the privilege against compelled testimony; and *(2)* the act of production doctrine. While the Sixth Circuit has provided limited protection to private papers under the Fifth Amendment, the clear trend of courts is that voluntarily produced papers of individuals have no Fifth Amendment protection.[80] However, where the act of production constitutes a testimonial compulsion protected by the Fifth Amendment, despite the contents not being protected, courts have extended Fifth Amendment protection.[81] The theory is that the act of production through the culling of records is "testimonial" in effect and, therefore, protected.[82]

After an individual receives a grand jury subpoena, civil investigative demand, or other compulsory process, counsel for the individual must determine whether to assert the Fifth Amendment as to each item. The relevant factors to consider are *(1)* the client's criminal exposure, *(2)* the impact of the information requested on the client's criminal exposure, *(3)* the available use, derivative use, or transactional immunity, and *(4)* the impact of non-cooperation on the government's choice of forum (i.e., criminal, civil, or administrative). Balancing these

considerations, it is important to determine if non-production citing Fifth Amendment concerns is the best option. Given the similarity of health care criminal statutes and administrative regulations, health professionals often face criminal culpability when responding to government investigations. However, failing to produce documents pursuant to a civil investigative demand citing Fifth Amendment concerns may cause federal investigators to seek alternative, more uncomfortable modes of production. Prior to citing Fifth Amendment concerns, counsel should discuss the scope of the request with the entity seeking the records and attempt to satisfy the requestor with as much information as possible while making Fifth Amendment concerns clear. A simple responsive document failing to produce any records and citing one privilege after another is not likely to produce the intended result, being a swift end of the investigation for the client.

Production

After all relevant information has been gathered and has been assessed for privilege considerations, relevant responsive documents must be produced. Prior to production, lead counsel should carefully review the response, privilege log, and responsive documents to ensure they comply with the request and are accessible. All documents must be indexed or bates stamped in order to easily identify the document, and the format should be used throughout each successive production. All documents must be produced in a commonly utilized format (i.e., .WMV, .PST, .PDF). Word documents should be converted to .PDF files in order to avoid modification. Counsel may contact the requesting party to determine what format the requestor recommends.

Accidental Destruction

Inevitably, emails are deleted, data is lost, and some individuals destroy information in order to avoid disclosure. Actual or attempted alteration, destruction, or concealment of a document or a record is a violation of 18 USC 1519 and is a felony punishable by up to 20 years

in prison. It is important to note that this statute prohibits the "concealment" of a record which can include a broad range of conduct. In order to avoid such a mishap, a corporation should develop a strategy to deal with document retention and have a clear destruction policy that can be modified in the event of a preservation request. The policies should be clear to all employees and regularly updated. In addition, the policy must be strictly enforced across all levels of the organization. Failure to enforce a policy is worse than no policy at all because it indicates knowledge of wrongful conduct.

B. Responding to Search Warrants

Health law practitioners service a broad range of clients and, from time to time, even attorneys that do not practice criminal law are likely to receive a frantic phone call from a client who is the subject of a search warrant. Knowing exactly what to say to a client in those crucial moments can make a considerable difference in the outcome of the case.

Before discussing what to do with the client, it is important for counsel to confirm that the government act is, in fact, a criminal search warrant. Some agencies, such as the DEA and FDA, possess administrative inspection authority to inspect the premises of an entity without first receiving a criminal search warrant. Often, these agencies present the client with a notice of inspection and seek access to the business. If inspection is refused, the agency can present a judge or magistrate judge with an administrative inspection warrant that will permit access, and refusal to permit access pursuant to an administrative inspection warrant may be grounds for arrest and contempt charges.[83] In this instance, counsel may make contact with the agency and attempt to schedule the administrative inspection at a later date – most entities will agree, but if it does not, it might be an indication that the agency has significant concerns or that it is not a random inspection. An administrative inspection is usually handled quietly with a few investigators approaching the front desk and asking to speak to the person in charge. If the inspection is

underway, counsel's role is to ensure the client cooperates with the inspection and to ensure that the investigators stay within the parameters of their inspection authority.

If the reason for the governmental presence is a search warrant and not an administrative inspection, the government will likely control the situation and will permit a phone call to be made to counsel only upon specific request of key personnel. Key personnel should be instructed to immediately call counsel upon any interaction with the government and have counsel's phone number handy in case of emergencies. Once that line of communication is open, counsel can request to speak with the lead agent and attempt to gain details about the search and determine the identity of the prosecutor assigned to the case. Most agents will agree to speak to counsel on the phone to inform counsel if any individuals are going to be arrested and to provide contact information for relevant government personnel.

Counsel should request a copy of the search warrant which will provide the case number, the magistrate and prosecutor assigned to the matter, and the type of information likely to be seized, but it will not provide a description of the probable cause for the search. Probable cause information can only be found in the search warrant affidavit, which will likely remain under seal and will be produced in discovery later.

Personnel on site during an inspection should be instructed to observe and write down important information about the search, including the questioning of witnesses, extraction of computer data, particular items searched and seized, agencies conducting the search, seizure of potentially privileged information, and length of the search. Next, an inventory of the company property seized must be obtained prior to the agents leaving the site of the search.

The government may also attempt to conduct employee and patient interviews on site during the execution of the search warrant. During DEA searches, it is common for diversion

investigators to enter the premises feigning an administrative inspection in order to obtain a statement from a registrant and then send agents in to bust down the door at the conclusion of the interview. The registrant would then be sat down for a second interview, which would likely be drastically different than the first.

Other agencies, such as the FBI and HHS, will enter the premises for a search with a pre-set interview plan and begin interviewing employees systematically. DOJ policy requires that agents must not conduct interviews of individuals whom the agency knows are represented by counsel regarding a particular matter. Thus, at the first hint of a government investigation, it is vital for counsel to retain an attorney who specializes in criminal matters in order to contact opposing counsel. If employee interviews are likely, the company can hire "pool" counsel to represent the employees during interviews and communicate that fact to opposing counsel. Employees should be instructed that they are not required to speak to the government, but if they choose to do so they must provide truthful answers.

C. Responding to a Civil Investigative Demand

Often, the first contact an entity has with the government is the receipt of a Civil Investigative Demand (CID). The False Claims Act permits the issuance of a CID as a means to obtain evidence in furtherance of a False Claims Act complaint. Other federal statutes permit similar investigative demands in securities, antitrust, consumer protection, and RICO investigations.[84] CIDs can seek written interrogatories, oral testimony through depositions, and the production of documents. CIDs requesting the production of documents are the most frequent. The DOJ has drastically increased its use of CIDs in recent years, reporting a six-fold increase according to the most recent estimates.[85]

There are many reasons the government may choose to proceed by way of a CID as opposed to a search warrant or grand jury investigation. In these cases, it is likely because the

government does not have a sufficient indication of culpability to convene a grand jury investigation or obtain probable cause for a search warrant. Moreover, by use of a CID, the government is able to signal to defense counsel that the government is interested in pursuing a civil investigation, and this may invite defense counsel to be more willing to approach settlement negotiations without the threat of criminal action.

CIDs are notoriously broad and, generally, government attorneys cast a wide net when requesting documents. Counsel may object to an overbroad CID by filing a petition to modify or set aside the CID.[86] The petition to set the CID aside should be filed in the district court in which the entity transacts its business or the individual resides. The petition must be filed within 20 days after the date of service of the CID, or at any time before the return date specified in the demand, whichever is earlier. 31 USC 3733(b) provides that the government shall not issue a CID that violates that standards applicable to discovery requests under the Federal Rules of Civil Procedure. Therefore, objections to the CID can include overbreadth, undue burden, and privilege, among other objections.

When faced with a CID, counsel should attempt to narrow the scope of the CID through negotiation with opposing counsel while maintaining the air of cooperation. This will open up dialogue with the prosecution and may be helpful in determining the target of the investigation and its scope. Traditionally, after negotiations related to the scope of the CID, the government will have a better idea of what types of responsive documents the target may possess and can issue a superseding CID that narrows the scope of the request and provides additional time to respond. During dialogue with the government, it is very important to remain cooperative unless negotiations are so broken down that a petition to set aside the CID must be filed – petitions to set

aside CIDs can be costly for the client and are rarely successful given the government's broad investigative authority.

D. Responding to Subpoenas

There are two types of subpoenas that the government may utilize during health care investigations, being an administrative subpoena or a civil subpoena. Naturally, an administrative subpoena signals the existence of an administrative investigation and potential adverse administrative action. A civil subpoena indicates the existence of an open civil complaint against the client or another entity. There are over 300 instances in which federal agencies have been granted administrative subpoena power in one form or another.[87]

18 USC 3486 permits the Attorney General, or his designee, to subpoena information pertaining to federal health care offenses. An administrative subpoena is generally not objectionable if it is authorized by Congress, it is for a purpose Congress can order, or the documents sought are relevant to the inquiry, such as, in this instance, the investigation of a federal health care offense.[88] Objections to the enforcement of an administrative subpoena may be based on a constitutional provision or a statutory provision protecting disclosure.

Constitutional challenges of an administrative subpoena usually stem from the Fourth and Fifth Amendment, and both challenges are unlikely to be fruitful.[89] In *Oklahoma Press Publishing Co. v. Walling*, the United States Supreme Court found that a subpoena does not violate the Fourth Amendment provided that it is not excessive and the information sought is relevant to the particular inquiry involved.[90] The DOJ does not need to make a showing of probable cause to issue an administrative subpoena, but rather, a "reasonable relevance" test applies.[91] Moreover, the definition of "federal health care offense" pursuant to 18 USC 3486 is broad and includes a wide variety of health care offenses. However, challenges to the breadth of an administrative subpoena can be successful where the subpoena requests information that has no reasonable relevance to a

federal health care investigation, or when the subpoena is issued for an improper purpose, such as a pretext for a criminal investigation, harassment, or to encourage settlement.[92, 93] If production of the requested information would violate privilege, is unduly burdensome, or is motivated by an improper purpose, counsel may attempt to quash the subpoena by filing a motion to quash in the district in which the individual resides or where the business conducts business.

E. Audits and "Silent Audits"

The first "contact" by the government in an investigation may be with the client's data and not the client. Medicare uses a series of contractors to run its program: these include the MACs which process Original Medicare claims, the Recovery Audit Contractors (RACs), and the zone program integrity contractors (ZPICs). HHS-OIG and CMS also have direct audit authority and state Medicaid agencies and other health care programs all routinely audit providers. Federal and state health care programs take a multilayered and redundant approach to auditing. As a result of HIPAA's standard electronic transactions requirements, and Medicare contractor reforms that established a common data warehouse, there is now a vast common data base of comparable claims and other information that these government agencies and their contractors rely on to audit and compare data. It is now possible to use ever-increasing sophistication in algorithms and artificial intelligence (AI) to extract information from vast numbers of claims and compare it to peers and standards. As a result, claims and all other submissions to the government, private insurers, and others (IRS, licensing agencies, etc.) are now available and being mined by the government and its contractors.

In many cases, the predicate for an investigation in the health care sector is the result of data analysis or audits conducted by any one of these agencies, contractors, or private insurers. Any provider that is experiencing audit issues or receiving a sharp uptick in requests for records or "Additional Document Requests" (ADRs), should escalate this activity to senior management

and the compliance department, along with counsel. Policies should be developed and employees trained to spot these trends and act accordingly.

F. Using Digital Data to the Client's Advantage

Do not be afraid of the digital age. The need to understand and effectively work with vast amounts of information in digital format has now become an essential quality for any health care lawyer that advises clients responding to investigations. If counsel does not understand their clients' technology and data, they should not be afraid of using an expert to work alongside them to help respond to the government.

Having a real handle on the data in response to an investigation can be a powerful negotiating tool. Here are several strategies for using digital data to the client's advantage:

- Start early, really early, right away! Clients often delay the production of digital data because they do not fully understand the request, they hope the lawyer will make it "go away" before they have to comply, and because they do not want to incur the expense. This is a mistake. Knowing the facts, which is the data, is essential to setting goals and strategies for responding to the government.
- Narrow the scope. At the very same time, counsel should be pressing the government to narrow and better define the scope of the request. This process can also help counsel better understand the government's position.
- Look at digital data in a new way. Do not try to make sense of the digital data the same way one would consider a contract or memo. Learn how to understand digital evidence or rely on an expert to help you.

- Do not rely too much on the client's IT department, they are not forensic digital technicians. Use a forensic IT expert when needed. Clients and their IT departments are often relieved to have a forensic expert assist in the production.
- Understand, prepare, summarize, and leverage data in responding to the government. Well organized and presented data can be a powerful tool in refuting the government, in self-reporting, and in negotiating satisfactory settlements. Use it.

G. New Department of Justice (DOJ) Standards for Conducting Investigations

In May of 2018, the DOJ adopted a new policy, ("Filip Memo") set out in the United States Attorney's Manual,[94] that requires greater coordination of investigations involving the same conduct and instructs DOJ attorneys not to use the threat of criminal prosecution to extract civil penalties, including CMPs.

The policy has four main elements. First, it reminds DOJ attorneys "not to use criminal enforcement authority unfairly to extract, or to attempt to extract, additional civil or administrative monetary payments."[95] Second, it recommends that DOJ components coordinate amongst themselves, where multiple DOJ components are investigating the same misconduct, in order to achieve a more equitable result. Third, the DOJ should coordinate with other federal, state, local, or foreign enforcement authorities seeking to resolve a case with a company for the same misconduct. Fourth, the policy requires DOJ attorneys to consider "all relevant factors" in determining whether multiple penalties serve the interests of justice in a particular case.

VI. Gathering and Preserving Electronically Stored Information (ESI) and Documents

Gathering, preserving, and producing Electronically Stored Information (ESI) and documents is one of the most important oversight tasks for counsel. Today, virtually all health care claims are electronic standard transactions, as required by HIPAA. Most claims' supporting

materials (*i.e.*, *CMNs, prescriptions, delivery tickets*), other scanned and faxed documents, e-mail and other communications are now electronically stored. As a result, most discovery in health care fraud cases involves electronically stored information or ESI as defined by the Federal Rules of Civil Procedure.[96] A prompt, well-coordinated and meticulous plan for preserving, gathering, and producing responsive ESI and documents is a major and critical part of representing the health care fraud client.

Although much of the actual production and preservation will be conducted by the client's staff and in particular, their IT and data departments, effective oversight by counsel is important for several reasons. In most cases, a team made up of operations, claims, IT, and any other recordkeeping staff should be assembled to respond, and the role of counsel to guide this team is pivotal. In addition to ESI, staff will need to identify and preserve any paper or hard copy records as well.

An important first step is to identify the resources available within the client's own office or organization to collect, preserve, and produce the ESI. Also identify any commercial software or data vendors the client uses to process and submit claims, store data or medical records, or perform accounting functions, and determine their ability to preserve and produce the data needed. If resources are lacking within the organization to identify, collect, preserve and produce records on a timely basis, it is essential to identify and engage outside data technicians, auditors, or others that can assist in the work so that it can be completed on a timely basis and without undue alarm and pressure on employees and staff. There are a number of "e-discovery" vendors that offer record preservation and production services and this should be explored with the client. Using an e-discovery vendor with experience responding to government investigations can make the process more complete, accurate, and timely; they can help produce data in formats that conform to the

government's formatting requirements and often it is cost-effective in the long run. Of course, any such engagement should be through counsel to protect the privilege and approved by the client.

Counsel should immediately identify the type of investigation and obtain all requests and demands for ESI and documents. Often the demands can be daunting – it is not uncommon for a CID to demand extensive data on an array of matters in very specific format. As described above, counsel will be instrumental in negotiating limitations to the scope of the request and the response time. Simultaneously, counsel and the organization must begin to take steps to preserve and prepare ESI and data for production. It is critical that preservation notices and steps be taken at the first sign of an investigatory demand for data. Doing so is not only required by law, it also demonstrates to the government the client's cooperation and good faith in responding to the investigation and allows counsel to begin gathering and analyzing the information the client will be required to turn over. Keep in mind, especially at the beginning of an investigation - "you don't know what you don't know."

The single most important factor in gathering and preserving evidence is to pay careful attention to what is being asked. Simply put, requests and demands can be lengthy, overbroad, and even obtuse. To a layperson, especially a data or claims technician, the legal language may be intimidating or misunderstood. It is critical that all requests or demands be carefully read and summarized to clearly identify the scope of the information needed, including careful attention to time periods, and that this information be effectively communicated to all staff, especially IT. Anyone supervising the preservation, gathering, or production of data and evidence should have easy and timely access to counsel for questions and guidance, preferably by phone or in person and not by email. Also, as counsel negotiates limitations on the scope or timing of the request or demand, that must be immediately communicated in clear terms as well.

The preservation activities and the notice will depend largely on the nature and scope of the investigation and the size and sophistication of the provider or organization. Obviously, the notice and preservation requirements for a small physician practice in response to a CMP will differ from that of a Medicare Part C plan or major health care system in responding to a *qui tam* action.

A. Preservation Notices

Preservation notices let employees and vendors know that an investigation is underway and that all ESI and other documents related to the investigation must be preserved and not altered in any way. It is important to strike a balance in this notice, it should not be draconian or overly alarming, and it should not detail the nature or extent of the investigation. The notice is about preserving the ESI and documents – not about the investigation. It is also appropriate and prudent to discuss the preservation notice with the government before its distribution.

The most important elements in any notice include:

- Clear and concise instructions that all ESI and documents subject to the notice must be preserved and must not be deleted, destroyed, or altered in any way.
- The consequences for failure to comply – including possible obstruction charges for any destruction or altering of ESI or documents.
- A clear and concise description of the ESI and documents to be preserved, including e-mails, text messages, instant messages, and off-site data.
- A clear and concise description of all the devices that the notice applies to, including personal devices that contain work related data.

- A clear and concise description of any equipment that the notice applies to. This may include fax machines, printers, and diagnostic or surgical equipment that store ESI.
- The time frame involved.
- Instructions to stop all routine data or document destruction.
- Instructions to suspend any backup media recycling and overwriting on cloud storage, mainframes, and stand-alone desktops and laptops.
- Instructions to suspend any auto-delete functions, including stand-alone devices. For example, 30-day automatic delete functions on e-mail applications should be suspended.
- Instructions for preserving ESI and documents going forward, especially any privileged documents.
- The individuals, contractors, and vendors covered by the notice. (Tip: review the accounts payable records to help identify all contractors or vendors that need to be notified.)
- The name and phone number of the person to contact with any questions or concerns, discourage the use of email for these questions.
- Encourage employees and vendors to take the notice seriously and to ask questions as needed.
- Instructions on how to handle privileged materials, and communications with counsel. (Tip: avoid the use of email for privileged communications, as staff often fail to place the attorney-client legend on them and can forward or share in a way that may compromise the privilege.)

- Ask vendors or contractors to provide a contact name and phone number for follow-up.

The single most important thing about the notice is to make certain that everyone receives it, reads it, and complies with it. This often requires follow-up to ensure that the preservation and gathering of information is implemented and maintained throughout the pendency of the investigation and case. Often investigations, negotiations, litigation, and *qui tam* cases can drag on for months into years. It is wise to renew the preservation notices from time to time, and whenever new demands are made or the scope or nature of the investigation changes.

B. Preserving ESI and Documents

Traditional preservation methods should be used for hard copy, paper documents, and tangible items. Originals should be identified by custodian and location and retained in secure storage; scans or copies should be made for review and production purposes. A detailed database or inventory of responsive documents should be maintained by counsel as work product, together with the location of all originals, and to whom scans and copies have been provided and when.

Preservation of ESI can be more challenging. Some ESI is stored in a medium that is readily accessible and can be obtained and read directly; examples include PDF scanned documents and emails. These can be simply downloaded and securely preserved in a separate data base or storage medium. Other times, ESI is stored in a format that requires translation into reasonably usable form to be read or studied. Claims processing and other data systems are examples of this type of ESI. Special care must be taken with systems that auto-update or delete certain information routinely in the normal course of business. Counsel must work closely and carefully with IT and any outside e-discovery vendors to understand, identify and preserve this type of data.

Preservation activities should include the following assessments and procedures:

- Identify and catalogue all computer hardware and systems: Mainframes, desktops, laptops and personal devices; operating systems and version; servers including exchange servers; removable storage medium such as thumb drives, CDs; and third-party storage, *e.g.*, "cloud" storage.
- Suspend all device and hardware disposals, including medical equipment, unless the data has been downloaded and preserved elsewhere, and maintain records of any such preservation.
- Ensure that all departing employees return all devices and storage medium.
- Identify and preserve all legacy systems not migrated to current system.
- Identify all applications and document management software, and preserve responsive data contained in these applications and software.
- Identify all email, instant message, voice mail, text message systems used. Identify the storage location of all and ensure preservation of all records; ask about and pay special attention to any auto-delete features or programs (*i.e.*, text messages automatically deleted after 30 days); and turn off or download and preserve records.
- Identify all document management systems, including word and PDF files.
- Identify all internet, intranet and web-based information and systems. Pay special attention to updates that routinely delete prior versions, such as websites. Use screen shots and other tools as needed to preserve prior versions.
- Identify and preserve social networking sites maintained or used by the client from deletion, or prepare a screen shot or other record.
- Identify any document cloud storage services used by the client, such as Dropbox or Google drive, and preserve relevant documents stored there.

- Identify all databases used by the client, their type and purpose, and understand routine reports, manuals, and how data is maintained and whether there are any auto-delete functions. Turn off any auto-delete functions and preserve data.
- Identify the client's backup systems and procedures and identify and review archived data.

The DOJ uses a comprehensive questionnaire in fraud cases to identify ESI and assess the adequacy of preservation efforts in health care fraud investigations.[97] Counsel and the client should be prepared to answer these questions when meeting with the government, especially in reference to any production of ESI or documents.

C. Special Issues – Employee Devices

Many companies and organizations now allow employees to "bring your own device" (BYOD) to the workplace. Smaller companies do this not only to accommodate employees' preferences for their own devices and ready access to social media and other personal information but to save the cost of providing these devices. In the health care sector, there is less tolerance for employee devices in the workplace, primarily due to HIPAA privacy concerns. Many hospitals and other facilities restrict the use of and access to personal devices for work purposes or even during work; however, many small practices, billing offices, and others allow BYOD. As a proactive measure, all health care providers, no matter how small, should consider providing work phones and other devices and requiring employees to use only those devices for work related communications and data.

In general, if personal devices contain material relevant to the investigative demands of the government, that information needs to be identified, downloaded, and preserved. This can be especially challenging on devices such as the iPhone where the user is the only person who can

unlock that data. Personnel and hiring policies, as well as record retention policies, should give the employer the right to access any data or information that is relevant to litigation or government requests. This is also an area where counsel for a provider or organization needs to be clear that they are not the employee's lawyer and be prepared for questions about whether the employee needs independent representation that may be triggered by the request for data from personal devices.

D. Record Retention Policies

The best defense is a good offense. A good records retention policy that is drafted with potential litigation and government investigations in mind; and that is understood and effectively implemented and maintained by executive, IT, claims, operation, and other staff is the best way to comply with any eventual demand or request by the government. Virtually every provider and health care organization will have to answer some type of audit, inquiry, or investigation by the government or a private insurer at some point, and often more than once. A records retention policy should address ESI and document storage, identify major laws and regulations, including time frames that apply to that provider or organization, and address what a litigation hold or investigation hold and preservation is in clear and understandable terms. It should specifically address the items listed above with respect to the stoppage of any auto-delete or routine data or document destruction. It should also address the use of personal or employee devices in the workplace. Finally, it should advise all employees and staff who they can contact with any questions or concerns about the policy.

Do not adopt a records retention policy that the client does not follow. One of the first things investigators will ask for is the client's records retention policy. Producing a policy that is not understood or followed by the client's IT or other staff is worse than having no policy at all. If the client is a small or mid-sized provider, it probably uses third-parties to provide claims

processing software or clearinghouse services or both, and for accounting, inventory, and other business functions. Give careful consideration to how the records retention policy is communicated to these vendors and what is in the client's vendor agreements when it adopts the policy. Prompt and thorough responsiveness by third-party data vendors should be considered before purchasing or using such software, servicing, or data storage.

VII. Production of ESI and Documents

Production of data and documents in response to the government is not a stand-alone job for counsel. It must be carefully coordinated with and integrated into the entire process of case analysis, client advice, goals, and strategies for addressing the investigation. For example, if the client is considering a self-disclosure or hopes for a negotiated settlement of the investigation, then the production should be timed to best support that strategy, if possible.

Counsel must be certain that they fully understand the scope of the request, the timing expectations, and the formatting and delivery requirements. The government will usually provide specific written guidance; for example, CIDs typically include an attachment with specific instructions for delivery, response, and formatting. In other cases, such as CMS letters regarding CMP sanctions, the request may be less intrusive or rely on data already reportable in CMS systems.

It is appropriate and useful to raise questions and concerns with the AUSA, HHS-OIG, or other investigators, while assuring the government of the client's intent to comply with the demand and cooperate (if that is the strategy). In fact, these discussions can also produce useful insights into the investigation and may result in narrowing of the request or an extension of time. Consider a staggered approach to responding; if the request covers a dozen facilities, offer to provide information on two of those for the government's initial review, or to provide information from a

shorter time period. As discussed above, be certain to have complete database record and accessible copies or scans of everything the client is producing.

Perhaps the most important thing is to be certain of is having a clear understanding of what the client is producing; this means actually reading or analyzing the documents and data being sent before they are produced. To accomplish this, counsel must start gathering documents and ESI as quickly as possible in the investigation and keep their foot on the pedal until everything is located and understood. The ESI and documents constitute most of the facts in the investigation. Counsel and the client must clearly understand these facts to analyze the risk and develop goals and strategies for responding to the investigation. Here again, the use of an e-discovery vendor can be very useful.

If expecting to self-report or negotiate a settlement with government, it can be very useful to retain outside counsel, and an independent review organization with experience in audits and reviews, to assist with data identification and review at this step. Self-reporting data and information that has been organized and reviewed by outside auditors and attorneys supports its objectivity and can be extremely useful in reaching a favorable settlement.

A. Format

The demand or request will usually lay out the formatting required for production. In general, the government will ask the client to produce original documents, but as a courtesy, will typically permit copies to be submitted. Of course, the originals must be kept and available for inspection. In reality, most responses are now entirely electronic. Privileged and lost or misplaced materials must be identified, although not produced, together with the explanation. Generally, documents are requested to be produced in electronic format, usually black and white .TIFF files, and all meta data such as hidden text must also be produced. All embedded files must be extracted and produced.

All documents must be produced with Bates numbers burned into each image. Specific instructions for the numbering may be included with the request and these should be followed carefully. ESI data and required metadata is also spelled out for each required field in the CID attachments. It is imperative that counsel and the client maintain a database or inventory of everything produced, the location of original documents, and the corresponding Bates stamp numbers. Even if the request does not specify Bates numbering, it is a best practice and should be used for any response.

All spreadsheets and power point presentation files must be produced unprocessed and as kept in the normal course of business. Instructions for production of emails, instant messages, and text messages are set out in the CID attachment and generally require the production of all logs and metadata associated with those communications.

It is important to understand the distinction between structured data and unstructured data. Structured data is represented by numbers, tables, rows, columns, and is usually transactional in nature. Excel spreadsheets, accounting ledgers, and claims data are all examples of structured data. It is usually numeric in nature. While structured data may include text, such as the name of a patient on a claim form, the text relates to the transaction. IT and data staff spend most of their time working with structured data. Unstructured data is often textual in nature; examples include emails, contracts, and medical records. Unstructured data can also include images, colors, sounds, and shapes. Examples include digital X-rays or other scans, graphics, drawings, and photos.[98] CIDs, and other government demands, address structured data and ask that prior to any production of data from a structured data base (SAP, SQL, QuickBooks, etc.) that the producing party provide the government with a database dictionary and list of all reports that can be generated, and specifies that the list of reports be provided in native Excel format. If the client requires any deviation from

the formatting instructions provided by the government, it is best to raise this with the investigators as soon as possible and work out a solution.

B. Timing and Scope

In a perfect world, every attorney and their client would have complete control over the timing of their production. Managing the timing of the production is one of the most challenging tasks facing counsel. As discussed above, timing is integrated with any strategies for defense, self-reporting, or settlement. The reality of negotiating the terms of production with the government, identifying and gathering the ESI and documents, and setting up the production runs from data bases are all largely out of counsel's control. Being an effective manager of the process or hiring and using an e-discovery service or expert, is critical to success.

Negotiations with the government over extensions can be useful. Do not just complain about the burden of production, but provide specifics about the challenges involved, while assuring the government of the client's commitment to producing the data and cooperating with the investigation.

The scope of the government's request or demand should be fully understood before any documents are produced. If counsel is unsure, ask for clarification; this can also help to better understand the government's position. Carefully establish and communicate the scope to everyone involved in the production process. Counsel should be sure to limit production to the actual scope of the demand. This sounds simple but knowing the parameters of the scope and sticking to them is often overlooked, as gathering and especially production of data from databases progress over time. Loop back to the original understanding of the scope on a regular basis and one last time before actually producing the client's ESI and documents.

VIII. Corporate Internal Investigations

After learning of an impending or actual government investigation, audit, or indictment, a parallel investigation or "shadow investigation" should be conducted. The origin of the internal investigation is rooted in the ability of corporate officers to avail themselves of the business judgment rule by investigating improper conduct and taking corrective action, and to obtain leniency in the event of enforcement action.[99]

Even after regulators have initiated an investigation or enforcement action against an entity, an internal investigation serves several important goals. Conducting an internal investigation satisfies management's obligation to investigate allegations of fraud. Additionally, if the internal investigation is initiated prior to actual knowledge of a government investigation or audit, the investigation may be used to self-identify the source overpayments pursuant to 42 CFR 401.305(g). Internal investigations also aid counsel in identifying and preserving documents and testimony that will be beneficial in negotiating with federal regulators. Finally, an internal investigation is vital to ensuring counsel gains detailed knowledge about the facts of the case in order to assess culpability. Counsel should not rely on receiving information from the government to assess culpability. Government investigative reports are often not disclosed until formal proceedings have commenced and are often one-sided, inaccurate, or misleading.

After the determination is made to commence an internal investigation, the first step is to determine the investigative team. Depending on the size of the corporation or the scope of the subject matter, the investigative team may consist of multiple attorneys, investigators, fraud examiners, accountants, statisticians, and medical experts. Otherwise, it may consist of just one attorney. Regardless of the size of the investigative team and the scope of the investigation, internal investigations proceed in much the same manner. Prior to beginning the investigation, careful thought and planning should go into the size of the investigative team and the practice areas

represented. For instance, if a hospice company is conducting an investigating drug diversion at one of its mid-size facilities, the investigative team may consist of two attorneys, an investigator, and an individual familiar with DEA compliance, such as a pharmacy consultant. While the majority of the investigative work should be conducted by attorneys to preserve the privilege, subject matter experts serve a vital purpose in identifying non-compliance.

When the internal investigation team has been compiled, a pre-interview meeting should take place to determine the scope of the investigation, interviews to be conducted, and documents or evidence to be gathered. Then, an investigation plan can be developed that lays out the components of the investigation and the roles of the investigative team. Investigations without a plan that is continually updated become unfocused and often fail to reach a conclusion. The plan should begin with a clear objective, timeline for completion, and final report date. The completion date will vary based on the urgency of the investigation. If the cause of the investigation was an anonymous tip reporting potential health care fraud, but counsel has no knowledge of the commencement of a government investigation, the internal investigation can be more detailed with an extended completion date. If the internal investigation was commenced pursuant to a civil investigative demand with a response date requiring production in the very near future, the investigation should be compressed and include a larger investigative team.

Whenever general counsel or independent counsel conducts an investigation and interviews employees, the employees should be advised that their statements may be considered privileged, but the company may reveal the statements at a later date, and that the company does not represent the employees' interests.[100] Moreover, if a conflict between the employee's and the company's interests is evident, the employee should be further advised to retain separate counsel. This advice should be given before the substance of the interview is revealed.

In *Upjohn v. United States*, 449 U.S. 383, 394-95 (1981), the Supreme Court adopted a test to determine if information provided by an employee should be privileged. In its test, the court considers the following: *(1)* if the employee's information was solicited for the purpose of providing legal advice to the corporation; *(2)* if the employee's information was needed by counsel to formulate legal advice to the corporation; *(3)* if the information was on matters within the employee's job duties; *(4)* if the employee knew the interview was for the purpose of legal advice to the corporation; and *(5)* if the employee's information was intended by the corporation to be confidential and, at least at the time of the interview, the corporation had no intention of waiving its privilege.[101] If the factors above are not met, according to *Upjohn*, the information provided by the employee would not be considered confidential and could be disclosed through compulsory production. Warnings to employees must be consistent with *Upjohn* in order to meet the Supreme Court's five-factor test and uphold the confidentiality of statements made to counsel.

After counsel has considered the necessity of *Upjohn* warnings and separate counsel, interviews of all employees who may provide relevant information should be conducted. Interviews of employees serve several functions: *(1)* to identify other documents and witnesses that are relevant to the investigation; *(2)* to collect information to advise the corporation on its culpability; *(3)* to preserve witness testimony for later use during government negotiations or court proceedings; *(4)* to allow management to fulfill its duty to conduct a thorough investigation; and *(5)* if possible, to make first contact with witnesses prior to the conduct of government interviews. Witness interviews should be conducted as early as possible and preferably before government investigators have had the ability to speak with the witness. Counsel should consider utilizing an investigator to be present for the interview in the event a witness is later cross-examined and impeachment testimony is necessary. However, investigators should not conduct most of the

questions, as investigators often lack the appreciation for the legal nuance involved in complex health care investigations. Counsel and the investigator should record the interviews, preserve all notes, and draft a report of each interview in a memorandum fashion clearly marked as "privileged." If the employee witness provides particularly exculpatory information, counsel should consider obtaining an affidavit from the employee.

When determining who to interview, counsel should begin with the individuals who have the closest proximity to the subject of the government investigation. This will ensure that other individuals who may possess knowledge can be quickly discovered and added to the interview plan. Counsel can always re-interview important witnesses after additional facts are gained from further interviews or to clear up conflicting testimony.

IX. Practical Proactive and Reactive Policies

The government relies strongly on a "sentinel effect" to prevent and detect fraud by avoiding or recovering improper and fraudulent payments. The government's approach has two primary components: prevention and recovery. Everyone in the health care sector knows that submission of fraudulent claims to any government program can result in severe criminal and civil penalties, including exclusion from health care programs. In addition, the government both requires and encourages self-monitoring and self-reporting of any improper payments, whether fraudulent or not. Some of the specific tools and programs to accomplish this are described here. Helping clients to understand these tools and how they can best be used in both proactive and reactive ways is an important role for health care counsel and compliance professionals.

A. An Effective Compliance Program

An effective compliance program is a proactive measure that can reduce fines and penalties resulting from health care fraud investigations and prosecutions by reducing the organization's culpability score. The United States Sentencing Guidelines[102] provide for reduced criminal fines

and penalties for organizations, including health care organizations, that have implemented an effective compliance program prior to the offense. The OIG, for example, will consider the existence of an *effective* compliance program that pre-dated any governmental investigation when addressing the appropriateness of administrative penalties. Further, the False Claims Act provides that a person who has violated the FCA, but who voluntarily discloses the violation to the government, in certain circumstances, will be subject to double, as opposed to treble, damages.[103]

Moreover, an effective compliance program can actually prevent investigations and *qui tam* cases in the first place. By identifying and correcting improper payments, responding to hotline and other complaints, and monitoring and self-auditing compliance with program requirements, an organization may prevent an investigation from ever happening. The government also takes into account whether or not the organization has an effective compliance program in place when making the decision whether or not to prosecute or impose penalties.[104] Monitoring and auditing under a compliance program is essential to complying with federal overpayment or "reverse false claims" requirements, and to identify and self-report any violations of law or CMPs before an investigation begins. By returning overpayments on a timely basis, and self-reporting violations, an organization can significantly reduce CMPs and other penalties.

An effective compliance program must include all seven elements found in the Sentencing Guidelines:

- Written policies and standards of conduct.
- Compliance officer, compliance committee.
- Effective training and education.
- Effective lines of communication, hotlines.
- Enforcement through disciplinary actions.

- Monitoring and auditing.
- Prompt response and corrective action.

An effective compliance program demonstrates to employees and the community that the organization is committed to honesty, ethical behavior, and acting responsibly; it encourages employees to report problems; it creates a process by which the organization can identify and prevent criminal and unethical conduct. It can also help to identify and correct compliance problems before they are discovered by the government or reported by a whistleblower.

The HHS-OIG has published Compliance Program Guidance[105] for a number of health care industries, including hospitals, physicians, nursing facilities, hospices, home health agencies, clinical laboratories, durable medical equipment suppliers, and Medicare Advantage organizations. The HHS-OIG guidance for your client's industry type should be carefully reviewed and used in developing a compliance program. If no guidance exists for your client, consult the guidance for similar provider types.

B. Response Policies and Procedures: Standing Response Team

Every health care provider and organization should have some type of written policies and procedures for responding to government audits and investigations. In small organizations or provider offices, this may be a policy to bring all communications from auditors and the government to the owner, who can then work with their lawyer before responding. In larger organizations, the policy and procedure may involve the compliance officer or committee, in-house counsel, internal audit, IT, and others. All employees should know what to do if the FBI or other investigators appear on the premises, especially if there is a search warrant involved. Employees should also be educated, and shown letterhead examples, of the various types of requests they may receive in the mail and know where to direct the request or demand. Any

employee that responds to additional records requests (ADRs) or other record requests from CMS contractors or the government should be trained on what these requests are, how to identify them, and when to escalate a particular request before responding. Knowing when any such request must be handled or escalated immediately is an important part of the policy and training.

Larger health care organizations should have a standing response team, made up of senior executives, IT directors and staff, compliance staff, claims, and finance personnel. In-house counsel should serve as a pivotal member of the team, and outside counsel should be consulted and brought in immediately where there is no in-house counsel. The standing response team should receive routine training on audits, investigations, and escalation policies on an ongoing basis. The team can then be activated and start working on responses immediately upon receiving a government request or demand.

C. Reverse False Claims – Overpayment Return Requirements

In 2009, Congress extensively amended the FCA, and added a reverse false claims provision, making it a violation to "knowingly conceal" or "knowingly and improperly avoid" an obligation to pay or transmit money to the government.[106] In 2010, the Affordable Care Act went on to add a requirement that any Medicare or Medicaid overpayment must be reported within 60 days after the date on which the overpayment was identified.[107] Any overpayments not reported after this time, may create CMP liability and can be a violation of the FCA resulting in treble damages and steep fines.

CMS defines an overpayment as "any funds that a person has received or retained under" Medicare "to which the person...is not entitled".[108] It requires the person to report and return any overpayments that have or should have been identified by the "exercise reasonable diligence" standard in accordance with CMS instructions.[109]

It is important to distinguish between an "improper payment" or overpayment and a violation of the FCA, AKS, Stark Law, CMP laws or other applicable laws. An improper overpayment means a payment that was received in error – whether the error was made by the provider or the government. For example, if a routine revenue reconciliation shows that the MAC made duplicate payments for a series of claims, that is a reportable overpayment. On the other hand, if a provider became aware of the overpayment and failed to report it within 60 days, that becomes a violation of the False Claims Act. Generally, overpayments are reported to CMS and potential violations of law are reported to the OIG.

Counsel and the compliance officer must take a proactive approach to over payments and educate appropriate staff to identify and promptly report any overpayment to the compliance officer or senior management. Counsel should be used or engaged to oversee the reporting and repayment of any overpayments. The process for reporting overpayments is set by CMS and it differs greatly from the HHS-OIG Provider Self-Disclosure Protocol described below.

CMS requires that any overpayments must be reported within 60 days using an applicable claims adjustment, credit balance or self-reported refund.[110] The report of an overpayment is generally made to the applicable Medicare Administrative Contractor, and the provider generally has 6 to 8 months to fully identify and refund any overpayments. If your client is unable to make the refund it is important to contact the CMS contactor immediately to make arrangements. The overpayment lookback period is six years.[111]

The Michigan Medicaid Provider Manual sets out the process for reporting and refunding any overpayments at section 12.4, it simply requires documentation of the overpayment and a check for repayment.[112]

D. HHS-OIG's Provider Self-Disclosure Protocol

The Provider Self-Disclosure Protocol (SDP) establishes "the process for health care providers to voluntarily identify, disclose, and resolves instances of potential fraud involving Federal health care programs."[113] It was first published by HHS-OIG in 1998.[114] And in April of 2013, it was updated and republished to provide additional guidance to the health care community. The April 2013 SDP supersedes and replaces the prior SDP and all Open Letters that followed.

In keeping with its sentinel approach to program integrity, the SDP encourages self-reporting because it believes that all members of the health care community have a "legal and ethical duty" to deal with Federal health care programs with integrity.[115] The OIG provides the following benefits for disclosure: a presumption against requiring a corporate integrity agreement; lower multiplier on damages; and mitigation of exposure from the overpayment requirements of the FCA.[116]

All health care providers and suppliers who are subject to OIG's CMP authority can use the SDP. Providers and suppliers that make a disclosure are referred to as "disclosing parties." Disclosing parties who are already under investigation or audit are not automatically precluded from making a SDP disclosure, but they must do so in good faith.[117] The SDP process is only for disclosing potential violations of criminal, civil or administrative laws for which CMPs are authorized, this includes the FCA and the AKS. The SDP is not to be used for reporting overpayments which are generally reported to the MAC, or STARK law violations which are reported to CMS through its Self-Referral Disclosure Protocol.[118]

The disclosing party must specify the particular law and violation they are disclosing and acknowledge that the conduct being reported is a potential violation.[119] It is equally important that the disclosing party has taken corrective actions to ensure that the conduct has ended. It is

important for counsel and the client to identify the root cause of the violation and ensure that corrective action has been taken or is underway.

The SPD provides a detailed list of the requirements that must be included in the disclosure. Disclosures can be made online or submitted by mail. Where the disclosure involves the submission of improper claims, the disclosing party must conduct a review of the claims and provide a damage estimate. The SPD provides detailed guidance for this review and estimate. Of course, counsel and the client should retain the necessary outside auditors and experts to conduct this review both for the expertise and the objectivity that external auditors can provide.

Cooperation and a genuine desire to right the wrong is the essential element of the Protocol. This includes submitting all information on a timely basis, communicating through a consistent and highly responsive point of contact, and being willing to pay fines and penalties on a timely basis. The OIG states: "Disclosing parties who fail to cooperate with OIG in good faith will be removed from the SDP."[120]

The essential components of any successful self-reporting, disclosure or settlement of a government investigation are the following: Swiftly conduct an effective internal investigation, identify the root cause of the overpayment or violation, quickly develop and implement an effective corrective action plan, identify and quantify any overpayments, and refund any overpayments or fines to the government.

---

[1] While many of the concepts in this paper reference federal investigations, the strategies recommended in this paper are easily transferable to practitioners defending state health care investigations.

[2] *See e.g.,* 42 CFR 483.85 (long term care); 73 Fed. Reg. 56832, September 30, 2008 (nursing facilities); 70 Fed. Reg. 4858, January 31, 2005 (hospitals); 65 Fed. Reg. 59434, October 5, 2000 (small group practices).

[3] *See HHS Organizational Chart.* U.S. Department of Health & Human Services. Available at: https://www.hhs.gov/about/agencies/orgchart/index.html (last visited May 17, 2018).

[4] 42 CFR Part 1001; 42 CFR 1003.105

[5] 42 CFR Part 1003.
[6] Jean Stone. *Fraud, Waste & Abuse: What is HEAT Strike Force Doing?* Centers for Medicare & Medicaid Services. May 20, 2011. Available at: https://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Regional_Conference/2011/New%20York/Stonecolor.pdf (last visited May 17, 2018).
[7] Office of Inspector General. *Medicare Fraud Strike Force*. U.S. Department of Health & Human Services. Available at: https://oig.hhs.gov/fraud/strike-force/ (last visited May 17, 2018).
[8] Office of Inspector General. *Medicare Fraud Strike Force.* U.S. Department of Health & Human Services. Available at: https://oig.hhs.gov/fraud/strike-force/ (last visited May 17, 2018).
[9] 21 USC 801 *et seq.*
[10] Michigan Department of Health & Human Services. *Special Investigations Unit*. State of Michigan. Available at: https://www.michigan.gov/mdhhs/0,5885,7-339-71547_5526_7028_7064_75936-314409--,00.html (last visited May 17, 2018).
[11] MCL 333.16221 *et seq.*
[12] Department of Attorney General. *Health Care Fraud: Medicaid Fraud Control Unit.* State of Michigan. Available at: https://www.michigan.gov/ag/0,4534,7-359-82915_82919_82267_82302-447767--,00.html (last visited May 17, 2018).
[13] The Health Insurance Portability and Accountability Act of 1996 (HIPAA), 18 USC 24(b), amended the U.S. Criminal Code to include a general prohibition against health care fraud. It is important to note that it defines a health benefit program to include any public or private benefit plan or contract.
[14] 18 USC 1347, 1349 and 3571.
[15] 18 USC 982(a)(6).
[16] Department of Justice. *Office of the U.S. Attorney's Manual, 922. Elements of 18 U.S.C. §287*. (USAM). Available at: https://www.justice.gov/usam/criminal-resource-manual-922-elements-18-usc-287> (last visited May 16, 2018).
[17] 18 USC 287, 18 USC 3571.
[18] Effective on February 3, 2017. *See* 82 FR 9131, Feb. 3, 2017.
[19] Department of Justice. *Fact Sheet, Significant False Claims Act Settlements and Judgments.* Available at: https://www.justice.gov/opa/press-release/file/918366/download (last visited May 16, 2018).
[20] Originally applicable only to Medicare and Medicaid (Section 1128B(b) of the Social Security Act), HIPAA expanded the scope of the AKS in 1996 to other federal programs, including state programs that receive federal funds. The AKS does not cover the Federal Employees Health Benefits program.
[21] 42 USC 1320a–7a.
[22] *See also* 42 CFR Part 1003.
[23] 45 CFR Part 160 and Subparts A and E of 164.
[24] Department of Health and Human Services, Office of the Inspector General. *Civil Monetary Authorities.* Available at: https://oig.hhs.gov/fraud/enforcement/cmp/cmpa.asp (last visited May 19, 2018).
[25] 42 USC 1320a-7(c)(3)(B).
[26]Department of Health and Human Services, Office of the Inspector General. *Exclusions Authorities.* Available at: https://oig.hhs.gov/exclusions/authorities.asp. (last visited May 19, 2018).
[27] 18 USC 1001.

[28] 18 USC 1341, 1343.
[29] 18 USC 1961.
[30] 18 USC 1345.
[31] 18 USC 1956 – 57.
[32] Department of Health and Human Services, Office of the Inspector General. *State False Claims Act Reviews*. Available at https://oig.hhs.gov/fraud/state-false-claims-act-reviews/index.asp. (last visited June 4, 2018).
[33] United States Sentencing Commission. *Quick Facts, Health Care Fraud Offenses.* Available at https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Health_Care_Fraud_FY16.pdf. (last visited June 4, 2018).
[34] 42 USC §§1320a-7(a)(1)-(4).
[35] 42 USC §§1320C(a).
[36] Department of Justice. *Justice Department Recovers Over $3.7 Billion from False Claims Act Cases in Fiscal Year 2017.* Available at: https://www.justice.gov/opa/pr/justice-department-recovers-over-37-billion-false-claims-act-cases-fiscal-year-2017 (last visited May 19, 2018).
[37] *Id*.
[38] See, Fed. R. Crim. P. 41.
[39] 18 USC 3486.
[40] 42 USC 205(d); 1320a-7a(j).
[41] USAM 9-44.200 – 204.
[42] USAM 9-11.150 -152. Elements of 18 U.S.C. §287.
[43] *Id*.
[44] 31 USC 3733(a)(1).
[45] Department of Health and Human Services, Office of the Inspector General. *Civil Monetary Authorities.* Available at: https://oig.hhs.gov/fraud/enforcement/cmp/cmpa.asp (last visited May 19, 2018)
[46] *Id*.
[47] 31 USC 3730(b)(1).
[48] Department of Justice. *Justice Department Recovers Over $3.7 Billion from False Claims Act Cases in Fiscal Year 2017.* Available at: https://www.justice.gov/opa/pr/justice-department-recovers-over-37-billion-false-claims-act-cases-fiscal-year-2017 (last visited May 19, 2018).
[49] *Id*.
[50] USAM CRM 9-11.151.
[51] *Id.*
[52] USAM CRM 160. Available at: https://www.justice.gov/usam/criminal-resource-manual-160-sample-target-letter (last visited May 17, 2018).
[53] *See United States v. Wong,* 431 U.S. 174, 179 n.8 (1977); *United States v. Washington*, 431 U.S. 181, 190 n. 6 (1977); *United States v. Mandujano*, 425 U.S. 564, 573-75, 584 n.9 (1976); *United States v. Dionisio*, 410 U.S. 1, 10 n.8 (1973).
[54] USAM CRM 9-11.150. Available at: https://www.justice.gov/usam/usam-9-11000-grand-jury#9-11.150 (last visited May 17, 2018).
[55] *United States v. Mandujano,* 425 U.S. 181, 186 (1977).
[56] USAM CRM 9-11.151.
[57] Counsel should proceed in the manner more fully detailed in the section dealing with shadow investigations.
[58] More fully detailed in the section regarding subpoenas below.

[59] *See* MRPC 1.7 and 1.13(e).
[60] *Managed Care Solutions, Inc. v. Essent Healthcare, Inc.,* 736 F. Supp 2d 1317, 1324 (S.D. Fla. 2010).
[61] *Zubulake v. UBS Warburg, LLC,* 220 F.R.D. 212, 217 (S.D.N.Y. 2003).
[62] *See In re Vioxx Products Liability Litigation,* 501 F. Supp. 2d 789, 808 n.31 (E.D. La. 2007).
[63] Other privileges include the marital communications privilege, accountant-client privilege, clerical privilege, doctor-patient privilege, and psychotherapist-patient privilege.
[64] *Upjohn v. United States,* 449 U.S. 383, 387 (1981).
[65] *See generally,* Larkin, *Federal Testimonial Privileges,* 2.03 (11th Ed. 1992); *In re Grand Jury Proceedings,* 791 F.2d 663 (8th Cir. 1986) (collecting cases from other circuits); *see also Humphreys, Mosley v. Donovan,* 755 F.2d 1211, 1219 (6th Cir. 1985).
[66] *In re Grand Jury Proceedings (Gordon),* 722 F.2d 303 (6th Cir. 1983).
[67] *Id.*
[68] *Leibel v. GMC,* 250 Mich. App. 229, 241, 646 N.W.2d 179 (2002); *Franzel v. Kerr Mfg. Co.,* 234 Mich. App. 600, 616 (1999).
[69] *In re Lott,* 424 F.3d 446 (6th Cir. 2005).
[70] *United States v. Zolin,* 491 U.S. 554, 563, (1989); *see also People v. Paasche,* 207 Mich. App. 698 (1995).
[71] *Zolin,* 491 U.S. at 561.
[72] *Zolin,* 491 U.S. at 561.
[73] *Hickman v. Taylor,* 329 U.S. 495, 511 (1947).
[74] Fed. R. Civ. P. 26(b)(4)(B).
[75] *United States v. Roxworthy,* 457 F.3d 590 (6th Cir. 2006).
[76] *Kent Corp. v. National Labor Relations Board,* 530 F.2d 612 (5th Cir. 1976).
[77] *United States v. White,* 322 U.S. 694, 699 (1944).
[78] *Braswell v. United States,* 487 U.S. 99, 105 (1988).
[79] *Braswell,* 487 U.S. at 110.
[80] *Butcher v. Bailey,* 753 F.2d 465, 469 (6th Cir. 1985).
[81] *United States v. Doe,* 465 U.S. 605, 610 (1984).
[82] *Id. See also United States v. Hubbell,* 167 F.3d 552, 575 (D.C. Cir. 1999), aff'd 530 U.S. 27 (2000).
[83] 21 CFR 1316.07; *see also* 21 USC 880.
[84] 31 USC 3733(a)(1).
[85] Kevin P. Mulry. *Justice Department Increasing Use of Civil Investigative Demands*. Farrell Fritz, P.C. May 22, 2012. Available at: http://www.nyhealthlawblog.com/2012/05/22/justice-department-increasing-use-of-civil-investigative-demands/ (last visited May 17, 2018).
[86] 31 USC 3733(j).
[87] U.S. Department of Justice Office of Legal Policy. *Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities, Pursuant to P.L. 106-544, Section 7*. Available at: https://www.justice.gov/archive/olp/rpt_to_congress.htm (last visited May 17, 2018).
[88] *Doe v. United States,* 253 F.3d. 256 (6th Cir. 2001).
[89] *Id.*
[90] *Oklahoma Press Publishing Co. v. Walling,* 327 U.S. 186 (1946); *see also United States v. Powell,* 379 U.S. 48 (1964).

[91] *Id.*
[92] *See generally, In re Subpoenas Duces Tecum,* 51 F. Supp. 2d 726 (4th Cir. 2000).
[93] *Markwood*, 48 F.3d 969, 980 (6th Cir. 1995).
[94] USAM 1-12.100.
[95] *Id.*
[96] Fed. R. Civ. P. 37e.
[97] Department of Justice, *Questionnaire on Electronically Stored Information.* Available at: https://www.justice.gov/atr/questionnaire-electronically-stored-information (last visited May 20, 2018).
[98] Inmon &Nesavich, *Tapping Into Unstructured Data: Integrating Unstructured Data and Analytics into Business Intelligence* (Boston: Prentice Hall, 2008), p.2.
[99] *Aronson v. Lewis,* 473 A.2d 806, 812 (De. 1984).
[100] *Upjohn Co. v. United States,* 449 U.S. 383, 394-95 (1981).
[101] *Id.*
[102] United States Sentencing Guidelines Manual, 8B2.1 (2013).
[103] *See* 31 USC 3729(a).
[104] USAM 9-28.800.
[105] Department of Health and Human Services, Office of the Inspector General. *Compliance Guidance.* Available at https://oig.hhs.gov/compliance/compliance-guidance/index.asp (last visited June 4, 2018).
[106] 31 USC 3729(a)(1)(G).
[107] 42 USC 1320a-7k(d).
[108] 42 CFR 401.303.
[109] 42 CFR 401.305.
[110] 42 CFR 401.305(d).
[111] 42 CFR 401.305(f).
[112] Michigan Department of Health & Human Services, *Medicaid Provider Manual*, https://www.michigan.gov/mdhhs/0,5885,7-339-71551_2945_42542_42543_42546_42553-87572--,00.html (last visited June 4, 2018).
[113] Department of Health and Human Services, Office of the Inspector General. *Provider Self-Disclosure Protocol.* Available at https://oig.hhs.gov/compliance/self-disclosure-info/files/provider-self-disclosure-protocol.pdf (last visited June 4, 2018).
[114] 63 Fed Reg 58399 (October 30, 1998).
[115] *Provider Self-Disclosure Protocol*.
[116] *Id*.
[117] *Id*.
[118] Centers for Medicare and Medicaid Services, *Instructions for Disclosures of Noncompliance with the Physician Self-Referral Law Arising Solely from a Violation of 42 C.F.R. § 411.362(b)(3)(ii)(C)*. Available at https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/Downloads/Disclosures-Noncompliance-Instructions.pdf (last visited June 4, 2018).
[119] *Provider Self-Disclosure Protocol*.
[120] *Id*.