COSMOS
Navigate the Compliance Universe

Compliance Today - May 2023

Eric Hafener, MBA, CHC, CHPC (ehafener@northernlight.org, linkedin.com/in/erichafener) is Vice President of Compliance and Privacy at Northern Light Health, Brewer, ME.

Adam Turteltaub (adam.turteltaub@corporatecompliance.org, linkedin.com/in/adamturteltaub/) is Chief Engagement & Strategy Officer at Society of Corporate Compliance and Ethics & Health Care Compliance Association, Eden Prairie, MN.

Meet Eric Hafener: Experience on both sides of the fence

by Eric Hafener and Adam Turteltaub

AT: Before we get into the work you are currently doing as the vice president of compliance and privacy at Northern Light Health in Maine, I want to go back earlier in your career. You spent almost 25 years working for the US government. What led you to public service?

EH: After college, I briefly worked for a manufacturing company as an inventory control specialist. I liked the job but did not find it intrinsically rewarding. I had friends who worked in law enforcement and it seemed like an exciting, fulfilling career.

I spent the first five years of my federal career working as a U.S. Park Police officer in the Washington, DC area. This was a great opportunity to gain skills I would use throughout my career, particularly the ability to apply laws and regulations, investigate crimes, conduct interviews, testify in court, and establish rapport with a wide range of people. I enjoyed helping people when they were in crisis and the feeling that I was helping society. I was able to complete my Master of Business Administration during this period and after graduating, I began applying for special agent jobs.

After leaving the Park Police, I worked for a year as a special agent with the U.S. Department of Commerce, Office of Export Enforcement (OEE). The position was in OEE's headquarters and involved supporting field agents, developing leads, liaising with other agencies, working on policies and projects, and creating and administering training programs. I really wanted to be in the field conducting investigations and was fortunate to be able to transfer to the U.S. Department of Health & Human Services (HHS) Office of Inspector General (OIG) in Maine.

AT: What appealed to you about a position at OIG?

EH: There were several things that attracted me to the position. I liked the idea of investigating fraud cases, the position was located in Maine, and OIG agencies typically do not force their agents to relocate during their careers.

When HIPAA passed, it created the Health Care Fraud and Abuse Program, resulting in new criminal healthcare fraud statutes and increased funding to OIG and the Department of Justice (DOJ). As a result of that funding, OIG Office of Investigations (OI) opened suboffices throughout the country and hired a large contingent of agents. I was fortunate to be part of that group of agents and opened the first OIG office in Maine.

AT: What advice would you give others without investigation skills? How can they best develop them?

EH: Investigative skills can be developed through training. At OIG, we often hired auditors, accountants, clinicians, and others as agents, since it is easier to teach an auditor police skills than it is to teach a police officer to be an auditor.

At a minimum, there are two types of training I would recommend to anyone doing investigations, whether it is for compliance, risk management, human resources, or insurance fraud:

1. A general overview course on conducting investigations provides the basic foundational knowledge to conduct investigations. For many people starting out, their knowledge of investigations comes from television shows and movies, and basic investigative training can help build a framework within which to operate and correct any misconceptions.

2. Interview training, since there is so much more to interviewing than simply asking questions and writing down answers. In my opinion, interviewing is the single most important skill to develop as an investigator and yet it is often overlooked. I was fortunate to attend the Reid School of Interviewing and Interrogation after five years at OIG. By that point in my career, I had over 10 years of law enforcement experience and had been through two training academies. I thought I knew how to conduct interviews pretty well. I learned an incredible amount from the training and highly recommend it to anyone conducting investigations.

The Health Care Compliance Association (HCCA) and the National Health Care Anti-Fraud Association both provide excellent training for compliance professionals.

AT: Any specific do's and don'ts you found for conducting healthcare investigations?

EH: When first receiving a complaint, it is helpful to establish what laws, regulations, and policies may have been violated if the allegations are true. This will help determine the direction of the investigation, the information needed, and the questions that need to be answered.

Make sure to apply the law, regulation, or policy that was in place at the time of the violation. This is especially important if a significant amount of time has passed since the alleged conduct occurred, or if the conduct occurred over a lengthy period.

For billing matters, check local coverage and national coverage determinations and any other guidance from Centers for Medicare & Medicaid Services (CMS) and the Medicare carrier. For kickback and Stark allegations, check safe harbors, exceptions, advisory opinions, and the *Federal Register*.

Avoid jumping to conclusions. Perhaps your complainant has credibility issues, the subject of the complaint has a prior track record of wrongdoing, or the allegation sounds outrageous. Whatever the case, judgment should be withheld until sufficient information is obtained.

It is common for other issues to surface while conducting an investigation. While serious issues deserve attention, there is a balance between conducting a thorough investigation and getting distracted by irrelevant information.

Try to determine if there is any documentary evidence that could objectively aid and support your investigation, such as email, instant messages, text messages, security camera footage, audit logs, and time stamps.

Finally, remember that effective investigations involve fact finding. At the end of an investigation the facts either support or do not support the allegations. In some cases, there may be insufficient information to support a conclusion.

AT: Part of your work at OIG included acquiring digital evidence. With the ever-proliferating ways data is collected, stored, and shared, how can compliance teams best get a hold of all the data out there? Or is it now an impossible task?

EH: It is easy to get overwhelmed by the amount of data that organizations collect and store. From a compliance perspective, it's helpful to think of data from two perspectives—risk and opportunity.

Data storage presents two types of opposing risks to organizations—retention and privacy. Much of the data that an organization creates, acquires, and stores is covered by legal and regulatory retention requirements that obligate the organization to maintain the records for a minimum period of time. From a privacy perspective, organizations benefit when they maintain the least amount of data necessary to limit exposure from a breach. Establishing and maintaining a formal data governance process is an excellent way for an organization to help manage both types of risk.

Data also provides opportunities for compliance officers to identify issues and support investigations. Understanding the types of data available and how to access that data will greatly enhance the effectiveness of the compliance program. It is helpful to start with a big picture of the types of data that might be available:

- Revenue cycle data (coding, billing, charge master)
- Clinical records and data (electronic medical records)
- Financial data (cost reports, journals and ledgers, accounts payable and receivable data, credit card and bank statements)
- Human resource data (employee lists, payroll data, time and attendance)
- Computer data (computer logs, network logs, application logs)
- Communication data (email, instant messages, text messages, phone records)
- Government-provided data (Program for Evaluating Payment Patterns Electronic Reports, Targeted Probe and Educate letters, Comparative Billing Reports)

Once you gain perspective on the types of data that your organization maintains, you can begin to assess the degree to which you can use it to evaluate and mitigate risk, to conduct monitoring and auditing activities, and to aid in investigations.

AT: A related challenge is that with so much data, it can be difficult to determine the important data points and which ones are just noise. Are there any rules of thumb you go by?

EH: Developing a culture of compliance and nonretaliation where people can ask questions when things appear odd is vitally important. Compliance departments are usually a small part of any organization, and being able to leverage resources and empower employees and leaders to spot issues and raise concerns makes our jobs significantly easier. Encourage employees to be curious and question when things appear odd. This is especially important when there is a change in process or implementation of a new system. For example, a sudden sharp increase or decrease in department revenue following implementation of a new software platform should be a red flag that causes further review.

Risk assessments that are weighted for both likelihood and impact are valuable in identifying where to focus compliance and audit attention. While formal risk assessments are recommended annually, it is important to

monitor new and emerging risks on an ongoing basis. Monitoring the OIG work plan, government enforcement activity and guidance, and legal and regulatory changes can help identify new and emerging risks.

In some cases it is possible to automate compliance activities so that monitoring occurs in the background. For example, there are vendors with systems that automatically upload employee information on a recurring basis, allowing for ongoing federal and state exclusion monitoring.

AT: Let's move beyond data to wrongdoing in general. What were some of the common mistakes you saw otherwise legitimate healthcare providers making?

EH: Three common but significant mistakes I saw providers make are herd mentality, misplaced trust in larger entities, and fabricating records.

Herd mentality can also be described as "everyone else is doing it" and may manifest as "when I was at [insert hospital/health system here] we did this." Although there may be minor differences in coverage requirements from region to region, federal laws and regulations apply uniformly throughout the country. Several years ago, there was an osteopathic physician in New England who gave seminars on maximizing revenue for osteopathic manipulative treatment (OMT) visits through the use of modifiers. Unfortunately, the guidance he provided (using the -25 modifier to bill OMT in conjunction with an office visit) was incorrect and easily identified through data mining. Several osteopathic physicians followed his advice and were subsequently prosecuted under the False Claims Act (FCA).

Related to herd mentality is the notion that the activity of larger entities has been vetted by their legal and compliance departments and therefore complies with the law. This is common during contract negotiations and in individual encounters with vendor representatives and is frequently presented as "It must be ok to accept [*insert something of value here*] from [*insert large company here*] for [*insert conduct implicating Anti-Kickback Statute (AKS), Stark and/or bribery statutes here*] since they are a large national company and I'm sure their lawyers approved it." Educating leaders, contracting staff and providers regarding the AKS, Stark Law and federal bribery statutes, and advocating for early compliance involvement during negotiations can help address this risk.

At OIG, we encountered several instances of providers altering documentation in response to a subpoena or document request. The providers in these instances were attempting to make their documentation compliant after the fact. In some of these cases the underlying conduct being investigated would have at most resulted in a civil FCA case, but the subsequent alterations resulted in criminal charges. Typically, by the time a provider becomes aware of an OIG investigation there has been a significant amount of work already performed on the case and in some cases the OIG may already be in possession of some of the records being requested, either from patients or from cooperating employees.

AT: In August 2017, you left HHS to join Northern Light Eastern Maine Medical Center. What led you to try the other side of the fence? What led you to Northern Light, specifically?

EH: After 25 years in federal law enforcement, I was ready for a change. I had spent my entire OIG career in Maine, and became familiar with compliance officers and in-house counsel at most of the major hospitals and health systems. Over the years I had developed a favorable impression of Northern Light Health's compliance program. The organization was transparent in its dealings with the government and demonstrated that it took compliance seriously, so when I saw they had an opening for chief compliance officer at Eastern Maine Medical Center, I jumped at the opportunity.

AT: I imagine by then you had developed what you thought was a good sense of how compliance programs work. Were there any surprises when you took over the role and were running a compliance program?

EH: At OIG, we focused on billing fraud, kickbacks, grant fraud, and other types of fraud, but compliance work at an acute care hospital and a health system encompasses so much more. When I started at Northern Light Health, I was surprised at the breadth and scope that compliance entails. I also gained an appreciation for privacy risks and the importance of effective policies.

At HCCA's Basic Compliance Academy I saw a slide titled "Oversight of the Health Care Industry" meant to illustrate the extent to which providers are regulated.[1] The slide is a flowchart showing an individual—presumably a compliance officer—in the middle surrounded by multiple regulatory agencies. I would have never guessed that my job would include reviewing corrective action plans for ripped waiting room furniture and overseeing audits of posters in patient registration areas.

Privacy is a challenge in any healthcare organization, and it is hard to appreciate that until you are responsible for ensuring that thousands of employees comply with HIPAA. HIPAA privacy is a big risk area given that healthcare organizations often rely on entry-level staff that may not understand the impact of their actions. Unfortunately, these same people handle personal health information and interact with patients daily.

Finally, I have a much greater appreciation for effective policies and policy management. Well-written and organized policies help employees understand job expectations and help reduce the burden on managers and compliance officers.

AT:Let me flip that around. What do you think compliance professionals don't understand about OIG at HHS?

EH: There are four operational divisions within OIG: Audit (OAS), Evaluation and Inspection (OEI), Investigation (OI), and Office of Counsel (OCIG). OAS and OEI work is fairly transparent through the OIG work plan, and OCIG's Industry Guidance Branch produces OIG's compliance guidance, advisory opinions, fraud alerts, and other public documents. By contrast, much of OI's work is hidden from the general public.

OIG OI agents are federal law enforcement officers and investigate healthcare fraud, grant fraud, and federal child support cases. They receive training at the Federal Law Enforcement Training Center along with more traditional agencies such as Naval Criminal Investigative Service, Bureau of Alcohol, Tobacco, Firearms and Explosives, and the U.S. Marshals Service. Although they are criminal investigators, OIG agents also investigate civil and administrative cases involving the FCA, the Program Fraud Civil Remedies Act, and Civil Monetary Penalties.

Our "best" cases in the OI typically involved small providers without compliance departments or outright criminal enterprises whose sole purpose was committing fraud. In general, OIG and DOJ understand that large healthcare organizations serve important functions in their communities and this weighs into prosecutorial decisions regarding those organizations, particularly in rural and underserved areas. As an example, I investigated a substance use disorder treatment facility and identified criminal conduct on the part of the organization itself. Although we had sufficient evidence to charge the company criminally, the U.S. Attorney's Office pursued the case civilly under the FCA since a conviction would have excluded the organization and caused the loss of a vital service to a large Medicaid population.

This should provide comfort to compliance officers that discover wrongdoing on the part of their companies and are considering self-disclosure. Attempting to cover up an incident will often make matters significantly worse than if the organization discloses and cooperates in resolving the issue.

That said, it is important to note that both OIG and DOJ work hard to identify individuals within organizations who may have violated federal criminal laws and personally benefited from their conduct and will prosecute those people if appropriate.

AT: We are, we all hope, coming to an end of an era of vast pandemic-related changes to healthcare. In addition to all the negatives, did you see any positives for compliance programs coming out of the era?

EH: At Northern Light Health, I feel that COVID-19 helped break down silos and foster teamwork among different disciplines, compliance included.

COVID-19 provided an opportunity for federal agencies—particularly CMS—to reexamine their regulations and requirements, particularly around telehealth. Easing the legal and regulatory burdens associated with telehealth will increase patient satisfaction and treatment options while reducing risk by creating uniformity among payors.

COVID-19 has also created opportunities for compliance professionals to work in hybrid and remote positions, expanding career opportunities and improving work–life balance. The remote option works particularly well for companies that do not have an established physical presence, such as a telehealth-only company, and in positions involving a large amount of field work traveling to different onsite locations. I do feel strongly that there is a benefit to compliance officers being physically present, at least part of the time, in companies with physical locations such as clinics, hospitals, and office practices.

AT: How can we better prepare for future dramatic changes that we may not foresee, whether caused by a pandemic or other changes?

EH: It is hard to prepare for the unknown, but ensuring the compliance department is fully integrated into the organization and creating an ethical culture during normal times will help an organization during times of stress. Staying up to date on industry trends and changes happening generally in the healthcare industry as a whole can help provide a framework to understand and adapt to the regulatory schemes that will inevitably follow.

AT: Looking to the future, how do you see compliance programs evolving over the next five years?

EH: During my time at OIG, it was interesting to watch compliance programs evolve and mature from reactive, one-person departments to fully functioning, highly professional teams. HCCA has had a big influence on the development and growth of the profession.

COVID-19 sent shockwaves through a healthcare system that was already in transition. The entry of large national companies, like Walmart, into the healthcare sector and new technology startups capitalizing on the rapid growth of telehealth have stressed many traditional health systems and hospitals. This will lead to further mergers, acquisitions, and consolidation of hospitals and systems, the outsourcing of support functions such as revenue cycle and health information management, and new strategic partnerships between providers and insurance companies.

Effective compliance programs will be those that are appropriately staffed, can monitor and adapt to a rapidly changing environment, identify and respond to new risks and threats, and leverage resources and tools. Organizations are learning the hard way that understaffed, reactive compliance programs are ineffective and costly in the long run. Recent corporate integrity agreements require dedicated compliance officers that are not tasked with other duties.

AT: Thank you, Eric.

1 "Oversight of the health care industry (flowchart)," HCCAnet, June 14, 2012, https://community.hcca-info.org/hcca/communities/community-home/digestviewer/viewthread?GroupId=262&MID=13917.