

## HEALTH LAW CONNECTIONS

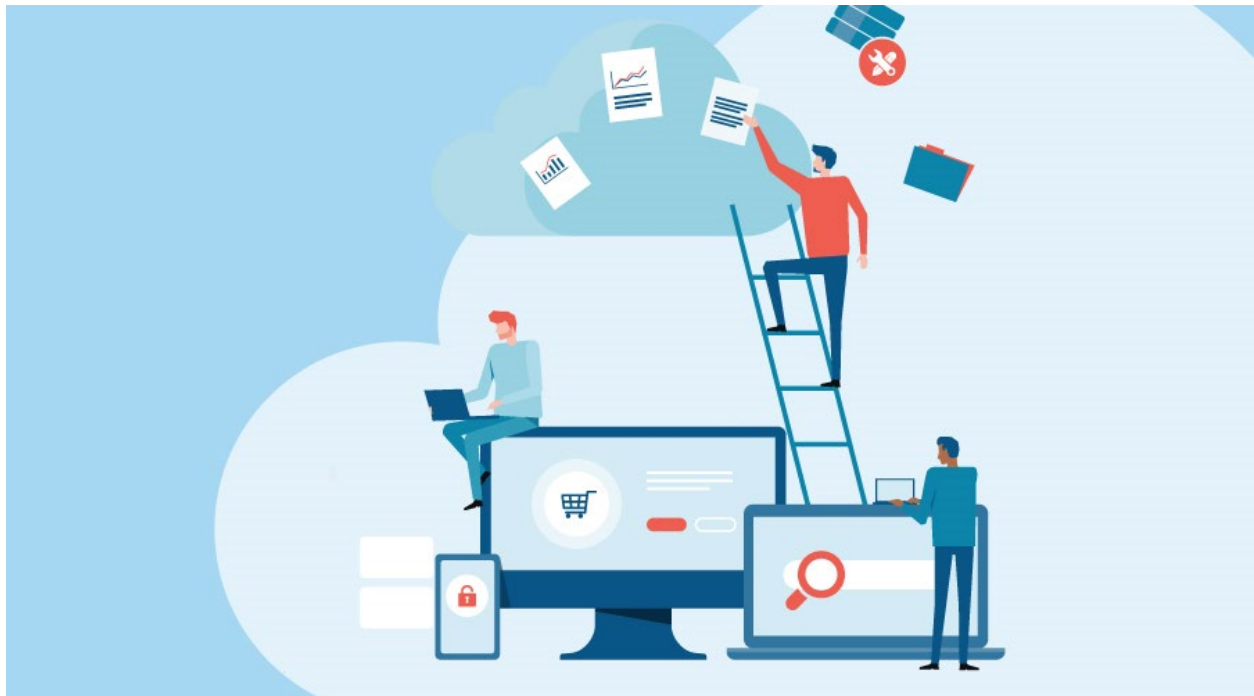
July 2022

# Better Handling of Electronic Communications During Government Investigations and Discovery: What Health Care Companies Can Learn from Other Industries

AHLA thanks the leaders of the Health Care Liability and Litigation Practice Group for contributing this feature article.

Pamela Johnston, Foley & Lardner LLP

Aaron Tantleff, Foley & Lardner LLP



In today's increasingly complex and ever-changing health care business climate, companies embroiled in government investigations or litigation often find themselves struggling to comply with Department of Justice civil investigative demands (CIDs), subpoenas, or document requests. Even under the best of circumstances, document collection, processing, and review are time consuming and expensive. Moreover, CIDs and document requests in false claims and other government investigations are often very broad and have unrealistic deadlines.

---

Copyright 2022, American Health Law Association, Washington, DC. Reprint permission granted.

This article discusses how technological tools adopted by other industries can help health care companies better position themselves to respond to such requests in a timely and cost-effective manner. It will also address:

- How to assist the compliance department in connection with further auditing and monitoring to avoid future problems;
- How mergers and acquisitions can raise the cost of data retrieval and productions, and how best to reduce those costs through full integration of the acquired company's data;
- When to avoid reviewing the records solely in-house before producing;
- How to advance the assessment of the merits through the document production process; and
- How to draw on insurance proceeds to cover the costs associated with document production in a False Claims Act (FCA) investigation.

## Enterprise-Wide Search Software Required in Other Industries

Advances in cloud software platforms have changed how companies archive and process emails, texts, key data, and share drive records. Certain financial industries, such as the broker-dealer industry, are obligated to use such advanced systems because the governing regulations require the company to keep and quickly produce certain documents to regulators, including key transactional documents and communications.<sup>1</sup>

Broker-dealers rely on platforms such as Brainspace Discovery, Commvault, IBM eDiscovery Manager, OpenText EnCase eDiscovery, Veritas, Google Vault, Exterro, and Smarsh, among others, to quickly search corporate email, instant messages, and share drives with Boolean logic or similar search methods to identify relevant communications and records. When responding to a CID, subpoena, or discovery requests, these platforms can quickly extract emails, instant messages, texts, and share records for review without restoring, collecting, and searching custodians' email boxes one by one. These systems also permit a user to rapidly and thoroughly search across a company's entire universe of electronic data, providing greater insight into the relevant issues.

While these platforms are more expensive than standard email systems, if a response to a large-scale request is required, the cost of these advanced systems is quickly recouped in the savings in attorney and paralegal time. Rather than using time-consuming, brute-force methods, company attorneys can review various subsets and clusters of records drawn from across the organization to test the issues and gather the key evidence quickly. In short, implementing an advanced software platform before litigation or receipt of a government CID can reduce the costs of producing records and enhance the ability to find the most important records relevant to the inquiry.

Furthermore, implementing such a platform allows a company's compliance department to receive real-time alerts about potentially problematic transactions and communications. Some industries deploy software with artificial intelligence (AI) that enables real-time analysis of communications and other data to identify behavior that may warrant corporate review or intervention. Corporate compliance officers can use AI tools such as Relativity's Trace or Smarsh to investigate the real-time communications that are often the precursor to a full-blown investigation or *qui tam* action.

When the law requires the use of such advanced systems, a company's failure to keep all communications on the company's system can subject it to sizable fines.<sup>2</sup> Even then, companies face the additional challenge of keeping their employees away from unmonitored mobile phones or alternative communication applications. This problem arises regardless of the official communication system used. Companies can limit such behavior by installing appropriate device software and by implementing and enforcing rules prohibiting side communications. While no method is perfect, it is usually better to implement a solution than to ignore the issue and hope for the best.

Many of these advanced platforms also partially automate—and significantly improve—the process of establishing a legal hold. This makes the initiation, dissemination, tracking, and enforcement of the holds easier and more reliable. These tools can easily show which employees received and read the legal hold notice, and promptly terminate the hold when the litigation or investigation is over. The legal and compliance departments will appreciate such automation.

Lastly, these advanced platforms permit health care companies to implement a standardized, company-wide electronic document retention plan. This is important particularly for companies that maintain legacy systems that contain previously archived data. The commonly accepted ten-year document retention hold policy may be too short to retain all required emails, instant messages, and claims data in connection with an unknown, sealed FCA *qui tam* action. A relator can file a FCA complaint under seal ten years after the claims were submitted to a government agency, if the government's knowledge of the violation was delayed.<sup>3</sup> Further, the complaint can remain under seal for years while the government investigates the claims. So, a health care company may need to access its own old records to defend itself more than ten years after the events at issue in the *qui tam* action. Memories fade and people leave, but old records can still tell the story years later if retained. Also, in some states, Medicaid contracts may require preservation of records for well past ten years, making the often-used ten-year preservation policy non-compliant and too short for practical purposes.

The portion of the health care industry that is currently not using advanced cloud-based enterprise platforms should therefore consider whether following the practices adopted by the financial services industry would be advisable for cost, compliance, and efficiency reasons.

## Acquisitions Can Intensify the Need for Advanced Enterprise Platforms

When a health care company acquires other entities, the acquiring company typically integrates the financial data successfully in short order. Yet many health care companies fail to plan for the full integration of the acquired company's prior email, text, and claims systems. These old systems are archived and often remain trapped in aging systems that are rarely maintained by the acquiring company's IT department. But when a lawsuit arises or a government CID arrives that requires the production of these archived records, then finding, reviving, and producing these old records can be especially costly, time consuming, and disruptive to the defense of the litigation or investigation. Too much attorney time is spent sorting out these archived records and reviewing them under less-than-ideal circumstances.

The lesson: The integration process can be better planned and executed if all of the data from the prior entity is brought over and integrated into an enterprise-wide platform shortly after the acquisition so that old data is not archived in an antiquated system. As with the adoption of cloud-based platforms, the upfront cost—while not inconsiderable—is more than recouped in just the first large-scale internal or FCA investigation.

## Enhanced Ways to Assist Compliance in Monitoring and Auditing

One of the long-term benefits of implementing an advanced enterprise search platform is that the compliance and legal departments can monitor and audit employee and company activities through the health care company's communications systems. Large, publicly traded health care companies have used these systems for years to help investigate legal and compliance issues. As the cost of such advanced systems has dropped and their sophistication and accessibility have improved, smaller health care companies can now afford to implement these systems. A compliance department can actively surveil the company's communications systems for regulatory breaches on a real-time basis and efficiently perform live searches in-house about budding issues.

This instantaneous in-house capability means smaller entities can do more than just audit claims and respond to complaints. They can set up automatic searches for key words (e.g., "call me, I don't want a paper trail" or "upcode") that can trigger an alert on a compliance officer's desk. They can proactively dive into system-wide issues with targeted searches. They can review text messages to see if a marketing employee, for example, is ordering impermissible lunches for third parties. They can filter the data to understand who has been talking to whom about an issue.

Tools like these can significantly enhance the compliance department's ability to monitor communications for worrisome issues. It can also simplify the production of reports needed for discussions with senior management. Of course, who can view data across the entire enterprise can and should be strictly controlled to prevent unauthorized persons from seeing sensitive data.

## **Risks That Arise When Records Are Solely Reviewed In-House**

When the time arises to review the records responsive to a CID, subpoena, or discovery request, health care companies should carefully consider whether the records collection and review should be conducted in-house. Different situations may give rise to a different approach to enable a complete response to the records request. For example, when responding to a routine third-party subpoena, it is common for in-house personnel to review the records for responsiveness if the size of the production is not extensive. If the subpoenaed health care company is a target of a government investigation, the government may be skeptical about the completeness of a production where the collection and production of records were conducted solely by in-house personnel. Similarly, reviewing records exclusively in-house in active litigation also poses problems when litigating responsiveness before a court. The courts often express skepticism of the completeness and accuracy of such collections, reviews, and productions.

Engaging outside counsel for these tasks may bring objectivity and professionalism in the eyes of the government or the court. Having the production reviewed solely by in-house personnel may reduce outside counsel's fees in connection with the production, but it may hinder defense counsel's knowledge of the documents and make it more challenging for counsel to develop a deep understanding of the records gained through the review of the communications. Defense counsel's lack of familiarity with the production may make the defense of the company more difficult: Issues and defenses can be missed, and nuances can get lost. It may ultimately increase costs because outside counsel will still have to review the production as the case moves forward. When the stakes are high, it is usually advisable to forego review for production by the in-house team in favor of employing outside counsel.

## **Discussing the Merits with the Government via the Document Production**

In most false claims investigations, it is worth discussing early with the government the issues that the CID seeks to explore. The government, however, frequently prefers to wait to discuss the merits of an investigation until all or nearly all the requested records are retrieved, produced, and reviewed. The government may postpone a discussion about the merits until the company produces all the requested emails, texts, and key documents so

that the government can rely on the key texts and emails relevant to scienter and other critical issues in such discussions.

This method is of course expensive and time consuming for the health care company under investigation. However, this approach can at times be sidestepped when the issues turn on legal questions or if the conduct is obvious, allowing all sides to dig into the merits of the case and look for opportunities for settlement before too much time and money has been spent. If possible, even when the conduct is not obvious, the defense should seek to vet issues about the merits with the government while the production is proceeding—tied to the production—to help the health care company test its theories before they need to be shared formally. This vetting usually advances later settlement discussions and allows both sides to understand more completely the contours of the various arguments that will be advanced during the discussion of the merits. It can also result in a narrowing of the records to be produced, leading to lower costs overall.

## Planning Ahead Regarding Insurance

Although insurance will typically cover the cost of discovery in litigation, it often does not cover the costs expended in response to a government CID or subpoena. A FCA investigation can be a major, and potentially catastrophic, event in the life of a health care company. Companies can seek to insure against the financial impact of such investigations. While an insurance policy likely cannot cover the payment of any penalties, it can help defray the cost of attorneys' fees and expert fees, which can be a lifeline to a smaller health care company. Yet many such companies are uninsured or underinsured for the risks created by a CID issued in a FCA investigation. But with advanced planning, a company can improve that situation.

The main barrier to coverage of a government investigation is how the standard policy is drawn: Most insurers require presentment of a financial "claim" before coverage is triggered. If the investigation commences by service of a CID, then a pending claim can exist but be "secret" because it is filed under seal. It is usually next to impossible to convince the insurer to accept coverage in this circumstance unless the definition of a "claim" has been broadened to include "investigative demands." To address this conundrum, it is worth exploring ahead of time with the insurance broker the cost of adding such language so that the arrival of a CID (a civil "investigative demand") will trigger payment of attorneys' fees and costs associated with the production of records and the defense of the case prior to any unsealing of the *qui tam* complaint. Even if an investigative demand rider is capped at a certain amount, the reimbursement can help with payment of some of the costs.

Next, it is worth exploring whether the health care company's counsel can convince the government to partially unseal the *qui tam* complaint as early as possible. Not every Department of Justice FCA investigation starts with the filing of a *qui tam* complaint. The government usually resists this partial unsealing step because it can potentially expose the

---

Copyright 2022, American Health Law Association, Washington, DC. Reprint permission granted.

identity of the relator, along with providing the health care company with insights into the pending allegations. But when the government can be persuaded to unseal (in part) a *qui tam* complaint, this may allow the health care company to present the “claim” to the insurer. Presentment of this sort can trigger access to the insurance policy for payment of reasonable attorneys’ fees and costs.

Finally, the last hurdle with many insurance policies is the type of attorney who can be hired. If a “standard” policy is accepted, the insurance company usually has the right to select counsel—and will rarely agree to pay for the retention of experienced false claims counsel. Here again, the upfront savings can turn out to be a chimera. Health care companies should address the selection of counsel with their insurance brokers ahead of time so all parties understand what type of lawyers—and their level of experience—the insured will be entitled to in a time of crisis.

## Conclusion

With advance planning, including the implementation of advanced enterprise software platforms, health care companies can reduce the lifetime costs encountered with the production of records in litigation and government investigations. These platform systems can also ease the burden of integrating the systems brought over from acquired entities and the compliance department’s ability to spot issues before they become full-blown problems. The nostrum “don’t be penny-wise and pound-foolish” applies in this context as much as anywhere else.

**Pamela Johnston** is a partner at Foley & Lardner LLP, who represents companies and individuals in investigations and cases involving the False Claims Act, health care fraud, complex criminal laws, and SEC/DOJ securities issues. Pam honed her trial skills during her 14 years as an Assistant United States Attorney, ending her Department of Justice tenure in the Los Angeles United States Attorney’s Office as Deputy Chief of the Major Frauds Section. She began that tenure as a civil AUSA prosecuting FCA, FIRREA, and forfeiture cases.

**Aaron Tantleff**, CIPP/E is a partner at Foley & Lardner LLP, where he represents companies in technology, privacy, security, big data analytics, artificial intelligence, information management, open source, intellectual property, and outsourcing matters. Aaron particularly focuses on the development of compliance policies and programs, cybersecurity breach preparation and incident response, big data, and data monetization initiatives across a wide range of industries, both domestically and in the EU and UK. Aaron has served as both in-house and outside counsel and served as the global director of IP for a global software company, and as acting AGC for a global information technology and management consulting company.

AHLA thanks the leaders of the Health Care Liability and Litigation Practice Group for contributing this feature article: Lindsey Lonergan, Navicent Health Inc (Chair); Oren Rosenthal, SCAN Health Plan (Vice Chair—Education: Publishing); Mackenzie Wallace, Thompson Coburn (Vice Chair—Education: Programming); Scott Grubman, Chilivis Grubman Dalbey & Warner LLP (Vice Chair—Education: Programming); Kara Silverman, Arnall Golden Gregory LLP (Vice Chair—Education: Publishing); and Kirstin Ives, Falkenberg Ives LLP (Vice Chair—Member Engagement).

---

## Endnotes

- [1](#) See, e.g., Securities and Exchange Comm’n (SEC) Rule 17a-4(b)(4) & (j) (codified at 17 C.F.R. § 240.17a-4(b)(4) & (j)); Financial Industry Regulatory Authority (FINRA) Rule 2210 (communications with the public).
- [2](#) See *In the Matter of J.P. Morgan Securities LLC*, Admin Proceeding 3-20681 (SEC Dec. 17, 2021 Order) (payment of a civil monetary penalty for failure to capture and keep required records).
- [3](#) 31 U.S.C. § 3731(b); *Cochise Consultancy, Inc. v. United States ex rel. Hunt*, 587 U.S. \_\_\_, 139 S. Ct. 1507, 1510 (2019).