What Health Care Organizations Need to Know about Electronic Discovery - Five Considerations That Should Not Be Overlooked During Healthcare Fraud Investigations

Jason Christ, Esq. Epstein, Becker & Green, P.C., Washington, D.C.
Jackie Flynn, UHY Advisors Discovery Services Practice, Washington, D.C.

Federal healthcare fraud investigations and enforcement actions have steadily increased in recent years. In 2009, the Department of Justice (DOJ) and Health and Human Services (HHS) formalized a joint initiative, the Health Care Fraud Prevention and Enforcement Action Team (HEAT), to prevent healthcare fraud and provide increased enforcement of ant-fraud laws. Under HEAT, a Medicare Fraud Strike Force was formed by creating a multi-agency team of federal and local investigators, analysts and prosecutors who utilized data analytics as well as conducted undercover operations to identify and expose the fraud. Since 2007 strike force operations in nine locations have charged more than 1,500 defendants who collectively have falsely billed the Medicare program.[1] In the Fiscal Year 2012, the government recovered a historic $4.2 billion and has returned a record-breaking $14.9 billion dollars to taxpayers between 2009 and 2012, up from $6.7 billion dollars over the prior four years.[2] These amounts have trended upwards over the past decade and in all likelihood will continue to do so. As part of the government's increased enforcement efforts, it is not unusual for healthcare entities to be the receipt of a Civil Investigative Demand ("CID"), Subpoena or Search Warrant once the investigation commences.

Those who have been through an investigation sometimes describe this time period as a black cloud that lingers over the institution until final resolution. These institutions often incur significant legal and electronic discovery provider fees, have difficulty raising capital, need to divert critical resources to assist counsel with response to the investigation demands and can even be suspended from government programs pending resolution. The investigation's outcome can depend substantially on the way in which an organization responds to a government demand. It is therefore in the entity's best interest to move quickly, yet mindfully, through an investigation.

Healthcare entities often wonder why electronic discovery ("eDiscovery") and production takes so long and is so expensive. Unfortunately, the pace of these investigations depends greatly on the scope and complexity of information sought by the government fraud enforcement entity(ies). The business of healthcare delivery is increasingly conducted today over e-mail and in specialized databases, which greatly increases the complexity of electronic discovery. For the vast majority of investigations, electronic discovery is therefore unavoidable.

Government enforcers often have jurisdictional guidelines based on their department's mission that require them to conduct a thorough and diligent investigation. For example, the Department of Health and Human Services Office of Inspector General (HHS-OIG) routinely investigates fraud in Federal Medicare and Medicaid programs while State Attorneys General may have jurisdiction to investigate health care fraud under their state law.[3] . There is much that counsel, working with experienced electronic discovery providers, can do to provide the responsive materials that are being sought by whichever government entity is conducting the investigation. A thorough yet strategic approach requires a full understanding of how healthcare investigations may differ from ordinary commercial litigation. The differences can pose some special challenges, but they also present opportunities to streamline production and move the matter forward to resolution.

THE GROWTH IN HEALTHCARE FRAUD WASTE AND ABUSE ENFORCEMENT

The U.S. Government Accountability Office ("GAO") has designated Medicare a high-risk area for fraud since 1990 because of its complexity and susceptibility to improper payments.[4] The Medicare program in 2012 covered more than 49 million elderly and disabled beneficiaries at an estimated cost of $555 billion and reported improper payments estimated to be more than $44 billion. Several factors are driving the increase in enforcement actions, the most significant of which is the increase in government-subsidized medical spending. The aging Baby Boomer population will drive increased healthcare spending as Americans live longer. Healthcare billing practices can be dizzyingly complicated, which makes them susceptible to fraud and mismanagement. Moreover, the government heavily regulates marketing practices through the Food and Drug

Reprinted from *ABA The Health Lawyer,* August 2014, Volume 26, Number 6.

Administration (FDA) while relationships with referral sources and reimbursement guidelines in clinical gray areas including medical necessity and reasonableness are regulated by Centers for Medicare & Medicaid Services (CMS)[5]. Finally, recent rule changes allow additional government designees to issue Civil Investigative Demands ("CIDs") more easily. "The Attorney General signed Order No. 3134–2010 (Jan. 15, 2010) delegating to the Assistant Attorney General for the Civil Division the Attorney General's authority to issue CIDs, and permitting that authority to be redelegated to other Department officials, including United States Attorneys." [6] A CID is a formal request from the government that may consist of a request for the production of documents, a demand for oral or deposition testimony, or a request for interrogatories requiring written response. CIDs are typically issued early in an investigation prior to a formal complaint being issued. The above and numerous other factors contribute to a robust enforcement climate and heightened risk for healthcare entities.

There are a myriad of federal and state enforcement stakeholders. Federal government enforcement agencies include, among others, the Department of Health and Human Services ("HHS") Office of Inspector General, Department of Justice, Federal Bureau of Investigation, Department of Veterans Affairs, Office of Personal Management, Department of Defense and various government contractors such as Recovery Audit Contractors ("RACs") and Zone Program Integrity Contractors ("ZPICs"). In addition, state governments bring their own enforcement actions against payors and providers typically using state versions of the federal False Claims Act.

CONSIDERATIONS THAT SET HEALTHCARE INVESTIGATIONS APART

From the outset, it is important to distinguish healthcare fraud and abuse investigations from traditional litigation. Federal- or state-based litigation occurs when a case or controversy exists and which one is initiated by a complaint. Healthcare fraud litigation can be initiated by a whistleblower complaint, called a qui tam action or a relator's complaint. Investigations and litigation can also be initiated by a federal agency or state government.

Not all healthcare investigations are litigation, at least in the traditional sense, since in many instances the government has not yet decided whether to pursue the matter. Moreover, many healthcare fraud and abuse investigations begin with a CID or subpoena, and proceed without the defendant ever interacting with a court and without the mandated formality dictated by the Federal Rules of Civil Procedure ("FRCP") or state civil procedure analogs. CIDs are a unique enforcement tool to obtain information as they are issued prior to a civil suit being filed and alleviate challenges to acquiring grand jury materials. Additionally, CIDs are commonly used by multiple government agencies providing oversight of highly regulated industries including health care as well as the financial services and government contracting sectors. This is not to say that electronic discovery in government investigations lacks discernible structure in attaining information. Indeed, quite the opposite can be true. But parties have flexibility in the manner in which they agree to proceed through the fact finding phase of an investigation. Notwithstanding this flexibility, below are important questions that health entities should ask their investigation counsel and electronic discovery providers.

ARE PATIENT DATA, PRIVACY AND SECURITY CONSIDERATIONS SUFFICIENTLY ADDRESSED?

Nearly all healthcare fraud and abuse investigations proceed on the hypothesis that a healthcare entity received or attempted to receive reimbursement from a government healthcare program in violation of a rule, statute or regulation. These investigations take innumerable forms but routinely involve conduct alleged to have violated laws such as: the Federal False Claims Act;[7] the various Civil Monetary Penalties under the Social Security Act;[8] the Anti-kickback Statute[9]; the Physician Self-Referral Prohibition, known as the "Stark Law"[10] and various other fraud statutes including the crime of Health Care Fraud.[11] Whether the conduct under investigation involves, for example, the provisions of services in the absence of medical necessity, violation of a billing rule or guideline, or a tainted relationship with a referral source, some form of patient claims data may be requested and examined by the government fraud enforcement entity.

This patient data can take numerous forms, including but not limited to: paper or electronic medical records; third-party payor billing records; coding records; patient coinsurance, deductible and copayment accounting records; and other patient demographic information. Patient data also exists in electronic mail and instant message platforms. Patient identifiable data and the organizations that handle this data are subject to a unique set of privacy and security laws and regulations. These privacy and security requirements must be carefully observed throughout the electronic discovery process. Data breaches that involve patient information can lead to separate government investigations as well as civil lawsuits filed by the affected patients. If a breach occurs during an existing government investigation, it could require the covered entity and its counsel to divert critical resources to mitigate the breach. It also seems

likely that such a breach could erode trust and confidence with government prosecutors and regulators at the worst possible time.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[12] and the Health Information Technology for Economic and Clinical Health Act ("HITECH")[13] are the most significant federal laws that govern the privacy and security of patient information.[14] The HIPAA Privacy Rule created national standards designed to protect medical records and other personal health information. According to HHS, "[t]he Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization".[15]

The HIPAA Security Rule establishes national standards to protect electronic personal health information ("PHI") created, received, maintained or transmitted by a covered entity[16] or its business associates[17]. The Security Rule "requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information."[18] HITECH, which was enacted in 2009, modified HIPAA by extending the Security Rule obligations to business associates, including lawyers and law firms that represent healthcare entities who are under investigation. It also increased the penalties for violations of any of these obligations. This means that all covered entities and their business associates must take measures to protect the security and privacy of patients' PHI, even if it has been requested in the scope of a government investigation.

Disclosure of relevant PHI is permitted for health oversight activities or for law enforcement activities under Sections 164.512(d) and 164.512(f) (respectively) of the HIPAA Privacy Rule. Section 164.512(f) permits a covered entity to disclose protected health information for a law enforcement purpose to a law enforcement official if certain conditions are met. Absent extenuating circumstances, as a practical matter, covered entities are permitted to disclose PHI to government enforcement entities who have requested the information in connection with a fraud, waste and abuse investigation. Despite this exemption, care must be taken only to transmit the minimum necessary PHI for government purposes and to ensure that materials are transmitted in a secure manner that protects them from third-party access.[19],[20] Finally, an additional burden remains on the entity disclosing the PHI in that the "the HIPAA Privacy Rule provides an individual with the right to receive a listing, known as an accounting of disclosures, that provides information about when a HIPAA covered entity discloses the individual's information to others."[21]

In January 2013, HHS issued a final rule under HITECH and HIPAA, which increased enforcement activity by the agency. The final rule includes notable enforcement changes that increase both the authority of DHHS and the risks for entities who handle PHI. Previously, HIPAA enforcement was complaint-driven, but under the HITECH Act and implementing regulations, DHHS will actively conduct HIPAA privacy and security audits as well as investigate entities that report data breaches. Additionally, HHS is now required to investigate all complaints where a "preliminary review of the facts indicates a possible violation due to willful neglect."[22] Given the enormity of PHI requested as part of the hundreds of annual fraud enforcement investigations, it seems like only a matter of time before a law firm or an electronic discovery provider mishandles PHI during eDiscovery and makes an already difficult situation much worse.

Healthcare organizations are not the only ones liable for data breaches. Business associates, including law firms and electronic discovery providers, may be subject to investigation and monetary penalties for failure to properly manage PHI. Electronic discovery tools, by nature, are designed to make information available for review and production. Accordingly, many were not designed with data security in mind. That means a conscientious approach must be taken regarding the manner in which law firms and electronic discovery providers receive, process, store and transfer data. It cannot be assumed that a law firm or electronic discovery provider is properly handling PHI and has taken every reasonable step to mitigate risk of breach.

Electronic discovery finds itself at odds with the principles of PHI security. Covered entities would normally avoid extracting vast amounts of PHI from clinical systems to external media for obvious reasons. But, this is precisely what eDiscovery often demands during an investigation. It is therefore extremely important for those under investigation to understand how data must be handled and ultimately protected.

From the outset, counsel and its electronic discovery providers should execute Business Associate Agreements ("BAAs") with the healthcare entity. This is essential. Among other covenants, these agreements require that parties comply with HIPAA and HITECH's privacy and security requirements. They should also clearly set forth the obligation of each party if patient data is lost stolen or otherwise compromised and obligate parties to com-

ply with the breach notification provisions under Section 13402 of HITECH and the corresponding Breach Notification Rule.[23]

BAA agreements with third parties accessing electronic information during an investigation are essential; however, they should not be mistaken as offering much by the way of protection. Organizations that manage health information should take additional measures, such as implementing encryption and security protocols, to protect that information from theft and unauthorized access.

The HITECH Act and implementing regulations require business associates to comply with the Security Rule. As part of that compliance, the Security Rule mandates that such entities conduct periodic risk analyses to identify and mitigate risks to PHI; therefore, counsel and its electronic discovery providers involved with healthcare projects should subject themselves to routine security audits and have established firm-wide PHI security protocols in place. Organizations may also consider seeking assistance from third-party auditors that can provide documentation of compliance with applicable security standards. This documentation will assist healthcare entities in vetting legal organizations that are prepared to securely manage their data during a government investigation.

Encryption for PHI stored on external or removable media is absolutely essential. Provided data is encrypted consistent with certain government standards, if it is lost or stolen the safe harbor principle under both HIPAA and many state data breach laws may apply. In certain circumstances the security incident may not need to be reported as a breach. Electronic discovery providers should use industry-accepted encryption standards such as FIPS 140-2 or NIST-validated encryption to safeguard all instances of PHI during collection, storage and transmission of client data. Types of encryption may be either software-based (for example TrueCrypt) or hardware-based (for example Data Locker) and vary in strength (for example AES 128 or 256 bit). Electronic discovery providers should also utilize secure FTP sites or other secure transfer protocols when sending or receiving data.

In addition, many healthcare organizations have installed organization-wide encryption across their IT networks to ensure data is protected via a software application or hardware level encryption for desktops and laptops. Such measures are not without drawbacks. Significantly, they can present logistical challenges when data needs to be reviewed or collected by an electronic discovery provider in response to a government investigation. For example, if a healthcare entity chooses to encrypt all of its hard drives, each hard drive will need to be decrypted to successfully collect the data and then re-encrypted for transport. This process can be time consuming and expensive. Outside counsel and electronic discovery providers need to be notified at the outset of discovery of any type of encryption used by the organization. This will enable counsel to have a more informed understanding of the timing associated with data preservation and ultimately production. It will also assist the electronic discovery providers with creating a more accurate time and costs estimate.

At times, the healthcare entity and its counsel may choose to allow certain custodians to self-collect data during discovery. This is not always an advisable strategy for a number of reasons, including the real possibility of mishandling data. Health entities and lawyers need to understand that data containing PHI should not be self-collected then shipped or emailed without taking measures to protect the data, especially encryption. If self-collection is deemed appropriate, custodians should be closely supervised to mitigate the possibility of mishandling. Some electronic discovery providers have remote collection tools that offer hardware-level encryption while allowing custodians to perform self-collection with minimal room for error. These types of providers should be engaged if self-collection will involve PHI.

Once the data has reached the electronic discovery provider, data that contains PHI may need to be segregated from other data sources within its environment. Electronic discovery providers may want to consider physically segregating cases with data sets that contain PHI on a separate server. They may also want to consider storing the data on a network without Internet access. Using software analytics and other culling strategies, sometimes electronic discovery providers can segregate and folder data containing PHI from other data sources within the document collection. This objective can be achieved using keyword searches, fuzzy searching, clustering like documents, grouping key concepts and prioritizing the data set using predictive coding or other forms of technology-assisted review. A skilled project manager can assist with this process, although this is not a foolproof technique and is limited by human judgment.

Electronic discovery providers should also limit the access of staff members to this type of information. This not only mitigates risk of inadvertent disclosures of PHI, but the Privacy Rule requires a standard of "minimum necessary" access for PHI. All members of the team should be asked to execute a confidentiality agreement that specifically addresses the handling of PHI.

When data is produced during the eDiscovery process, attorneys may consider removing "identifying" information by removing demographic information that links a patient to a record. This can be accomplished using redactions or deletion of PHI contained in the document collection prior to production. The process to exclude all PHI may become cumbersome since it often requires attorneys to tiff native files and manually redact the PHI portions. Deleting or redacting data is, unfortunately, rarely a possibility since the government may need the PHI to further its investigation. Moreover, documents are required to be produced as they were maintained in the normal course of business. Accordingly, counsel would be wise to seek approval from the requesting government agency and provide advance notice to any such document modification, even if performed with the good intention of minimize risk of breach.

WHAT ARE THE UNIQUE CHALLENGES OF DEALING WITH ELECTRONIC HEALTH RECORDS AND BILLING AND CODING PLATFORMS?

The healthcare community has increasingly embraced electronic health records ("EHRs"), database-driven clinical platforms, coding software and billing programs to create efficiencies and enhance care. These electronic platforms contain information that is often critical to government investigators. For instance, since government investigations often proceed on the theory that the healthcare entity has falsely billed for services, these software platforms are among the first places fraud investigators seek to examine. Moreover, government enforcement recently has moved toward investigating whether software defaults and pre-populated fields in EHRs may unlawfully increase reimbursement. In January of 2014, the OIG released a report that suggested that "EHR technology may make it easier to perpetuate fraud" and recommended that CMS and its contractors develop guidance and tools for EHR fraud detection and data mine using provider audit log data.[24] Coding platforms, too, have recently become highly relevant to the government since some of these tools can be programmed to make suggestions or prompt the user to select higher levels of service or codes. In such matters, the platform itself becomes the focus of the investigation.

EHR, coding and billing platforms, more often than not, are incredibly difficult to preserve, review and produce. There is no standard format for EHRs or coding and billing platforms, nor does it appear that the software industry designed these platforms with litigation and government investigations in mind. EHRs, by nature, are designed to limit access to and provide security of their records. Accordingly, easy export tools either may not exist or will provide only limited information. Many clinical platforms have a database mainframe backend, such as SQL or Oracle, which present its own challenges. Additionally, EHR platforms in particular may be organized as relational databases where information is organized and defined by a series of linked fields and tables. Preserving these databases outside of the system in which they operate is nearly always impracticable.

Counsel may attempt to resort to producing screen shots of requested data, but this arcane collection methodology is expensive, time consuming, and seldom provides a data set that can be easily reviewed, sorted and categorized in a manner that can advance the parties' objectives to resolve the matter. Moreover, screen shots are simply insufficient for the types of investigations where the platform and/or its programing itself are at issue.

Successfully working with EHRs during electronic discovery often requires counsel to have some technical experience, careful planning and a provider who can work with proprietary mainframe platforms. The same applies to coding and billing platforms. At times, the healthcare organization's team may be called upon to interact and coordinate with technical specialists on the government's team. Choosing the right team with this expertise is critical to control cost, promote efficacy, build trust and engage in fruitful discussions with the government and ensure the integrity of the data. Counsel can work with an experienced eDiscovery provider to extract data from the server and create reports to allow both counsel and the government to interact with the data in a meaningful fashion and work toward resolution of the underlying matter under investigation. These customized solutions are often the least expensive and most efficient option to move through the electronic discovery process for clinical systems.

WHAT DATA CHALLENGES CAN BE EXPECTED IN INVESTIGATIONS OF REFERRAL RELATIONSHIPS?

Fraud enforcement legislation such as the Anti-Kickback statute, the Stark Law and the Civil Monetary Penalties in the Social Security Act govern and prohibit certain financial relationships involving the transfer of remuneration (anything of value) between providers and referral sources in exchange for items or services that are reimbursable by certain federal programs including the Medicare Trust Fund. These relationships are regularly scrutinized by government enforcers during investigations. Accordingly, production demands often include

requests for any and all documents that pertain to remuneration to referral sources.

Healthcare organizations should keep in mind that responsive materials often exist in sources other than just the agreement between the provider and the referring entity. As such, government demands often involve large-volume email requests. Communication with referral sources through electronic mail is highly probable, though counsel and all electronic discovery providers should be more than capable of preserving, collecting and ultimately producing e-mail.

Increasingly, government demands include requests for specialized sales force data bases. Sales force records are certainly not unique to healthcare, yet they provide some of the most responsive and probative evidence of improper remuneration to referral sources in healthcare investigations. The temptation for sales force personnel, some of whom are compensated based on their individual productivity, to reward referral sources with items of value has proven too great, and is often accompanied by a propensity to document such rewards. As a result, there are a number of both civil and criminal settlements in which evidence of fraud was found, at least in part, on records created or maintained by sales force personnel.[25]

Sales force personnel have increasingly employed Customer Relationship Management ("CRM") systems. CRM databases are platforms that track interactions between the sales team and clients. Within healthcare organizations, CRM systems generally contain similar information but often include copies of proposals, contracts, notes and other critical documentation that details the nature of the relationship between the provider and its referral source. These systems may also track lunches, gifts and other free items given to a referral source.

CRM systems, like EHRs, are often database-driven. This means that all of the information an organization inserts into the system is ingested and stored in a database, not as individual, discrete documents. As such, counsel and electronic discovery providers must heavily leverage the CRM platform to ultimately meet government demands, including determining:

- What system is in place, such as Microsoft CRM or Salesforce.com
- How the individual organization uses the CRM platform
- The life cycle and hierarchy of a record
- What reports are typically run from the system in the normal course of business and what information those reports contain
- What process could be used to query and export information en masse
- How the data will be exported from the system and presented to counsel for review and ultimate production to the government

Counsel needs to plan carefully and work with the government on how to successfully produce this type of data. Despite broad government requests, electronic discovery providers seldom preserve and produce the entire CRM system. Even if entire systems are preserved, because they are accessed using customized, and non-standard software systems, the data that is preserved is typically unusable outside of the clients' environment. Running customized reports may be the best way to get the information needed to meet government demand; but, since only a portion of the CRM database will ultimately appear on a report, skilled negotiations with the government may be necessary to make this type of limited production possible.

CRM systems are not the only source of data that evidences interactions with referral sources. A more challenging problem is presented if the government requests accounts payable information related to sales force expense accounts and evidence of a direct payment to referral sources ("an AP run"). Many accounting systems that handle financial information, for example, a healthcare organization's general ledger, require technical expertise to preserve and collect structured data during the electronic discovery process. Like CRMs and EHRs, some accounting systems are web based, with the data residing on third-party servers. Many accounting platforms cannot be completely collected and still have information accessible for counsel's review since the data is useless outside of its web-hosted environment. Again, the preparation of specialized reports, although not legally required by subpoenas and similar government demands, may be an option to meet your eDiscovery obligation as an alternative to preserving the entire system. Based on the entity's accounting platform and reporting capabilities, more creative approaches may be necessary. In all circumstances, the technical experience of skilled healthcare counsel and its eDiscovery provider is critical to cost control and maintaining the integrity of financial data as it is being accessed and preserved.

WHAT ARE THE COLLECTION AND PRODUCTION CHALLENGES WHEN THE DATA REQUESTED INVOLVES A HEALTHCARE ORGANIZATION'S CONTRACTORS OR PHYSICIANS WHO ARE NOT EMPLOYED BY THE HEALTHCARE ORGANIZATION?

Another somewhat vexing anomaly in healthcare investigations is the confusion that surrounds the existence of affiliated providers. Externally, it may appear to government enforcers that the healthcare organization employs all of its clinicians and sales personnel. This is frequently not the case, especially for hospitals. Many physicians, nurses and technicians who ostensibly work in a hospital are in fact employed by a physician's practice or staffing company, not the hospital. Nonetheless, many contractors, including physicians, have access to or contact with sensitive information about patients and therefore may control data that may need to be preserved during an investigation.

For example, physicians with hospital staff privileges may have private email accounts used during the normal course of business. Third parties including the government may request this data, assuming that these e-mail accounts are in the custody or control of the hospital. Whether a requested item is in the custody and control of the entity subject to a document request is not always clear and experienced counsel often chooses to inform the government of the existence of third party data and engage the government in negotiations regarding its production. In circumstances in which the data is, in fact, outside of the custody and control of the healthcare organization under investigation, the healthcare organization should also determine whether it should inform the outside entity of the existence of the investigation, and extend notification to hold and preserve relevant documents, to ensure that data is not compromised. In some instances, such notification is a prudent if not necessary step; yet, in other instances, notice to a third party may compromise the government's investigation. Therefore, a careful and conscientious approach must be taken to data that is not clearly within the control or custody of the entity under investigation.

HOW CAN A HEALTH CARE ORGANIZATION ENGAGE THE GOVERNMENT IN MEANINGFUL DIALOGUE TO CONTROL COSTS AND PRODUCE THE MOST PROBATIVE EVIDENCE QUICKLY AND EFFICIENTLY?

The relationship between the government and the healthcare provider is particularly sensitive during fraud investigations. A confrontational approach is rarely recommended. This is especially so because, in healthcare investigations based on qui tam actions, the government is under an obligation to investigate and may not yet have decided whether to pursue the matter. In confronting the government early on, a healthcare organization may miss an important opportunity to convince the government to close the investigation and may invite other negative consequences. For instance, in healthcare investigations the government has the ability to suspend Medicare payments in certain circumstances and can choose to exclude individuals and entities from participation from federal healthcare programs. Application of these sanction authorities often depends on the extent of cooperation of the healthcare organization under investigation.

Skilled counsel will therefore treat regulators and investigators as they would treat a long-term business partner with whom their client disagrees, not necessarily as a pure adversary as in commercial litigation. Of course, this does not mean automatic acquiescence to government requests no matter how overreaching in scope or draining to organizational resources. What it does mean is that government demands will be treated with respect and a serious dialogue that attempts to deliver to the government information it needs to evaluate the matter while balancing the healthcare organization's need for reasonable cost and business continuation.

Building trust with the government can pay off in the long run. Counsel may choose to share the organization's legal hold notice and outline what data is being preserved in connection with the investigation. Sometimes data is no longer accessible, and healthcare entities and their counsel should be open and honest about what can be realistically done to locate the requested information.

In an investigation, the two sides are not mandated to hold a formal discovery meeting to discuss scope, volume and format of electronic discovery. However, a back-and-forth discussion with the government is in the healthcare entity's best interests. When negotiating, the legal team should try to limit and better define the scope of the investigation. The subpoena or CID may be broad in nature; in many instances investigators are at a disadvantage since they may not have an insider's view of the entity. It is counsel's responsibility to educate the government on where the most probative materials can be found and propose an electronic discovery plan accordingly.

Negotiating the scope of electronic discovery , as well as the production requirements, will also result in significant cost-savings across the life cycle of the matter. For example, the use of data found on an active e-mail server - rather than on hard drives and backup archiving systems - can significantly decrease the length and cost of electronic discovery. Hard drive and backup tapes are often budget breakers, but may need to be preserved and collected if there is not sufficient information on the active email server. This is often the

case where organizations allow only very limited volume on email boxes, so that people need to save documents to desk tops or external hard drives. Nevertheless, negotiating with the government to limit the scope of relevant email boxes can go a long way to control costs in these circumstances.

CONCLUSION

When the government initiates an investigation of a healthcare entity, the stakes are high, the issues are often complicated and the burdens to maintain patient privacy can be onerous. The legal team, including counsel and electronic discovery providers, cannot approach these cases as they would a typical litigation matter. They should establish a working relationship with the government throughout the eDiscovery process and develop an approach for cost containment while maintaining the security and integrity of the data.

ABOUT THE AUTHORS

Jason E. Christ is a Partner in Epstein Becker Green's Health Care and Life Sciences practice, in the firm's Washington, DC office. Mr. Christ concentrates in healthcare fraud and abuse, government investigations, and health regulatory counseling. He is a member of the adjunct faculty at American University Washington College of Law's Health Law and Policy Institute and is a coauthor of the American Health Lawyer's Associations Best Selling Book, *Legal Issues in Health Care Fraud and Abuse: Navigating the Uncertainties, 4th ed.* He may be reached at JChrist@ebglaw.com

Jackie Flynn is the Mid-Atlantic Client Services Manager for the UHY Advisors Discovery Services Practice. Ms. Flynn routinely consults with large domestic and international clients in the healthcare, telecommunications, technology, government contracting, energy and education industries with regard to formulating defensible collection plans, preservation strategies, data extraction, forensic analysis, targeted culling and document review. She may be reached at Jflynn@uhy-us.com

ENDNOTES

1 The United States Department of Justice, "Medicare Fraud Strike Force Charges 89 Individuals for Approximately $233 Million in False Billing," Tuesday May 14, 2013. http://www.justice.gov/opa/pr/2013/May/13-crm-553.html.

2 U.S. Department of Health & Human Services, "New Tools to Fight Fraud, Strenghten Federal and Private Health Programs, and Protect Consumer and Taxpayer Dollars," Accessed April 2014. http://www.stopmedicarefraud.gov/newsroom/factsheets/medicare-fraud.html.

3 The United States Department of Justice, "978 Health Care Fraud and Abuse Control Program and Guidelines," Accessed April 2014. http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00978.htm

4 U.S. Government Accountability Office, "GAO's 2013 High Risk Report", Accessed April 2014. http://www.gao.gov/highrisk/medicare_program/why_did_study#t=1

5 Centers for Medicare & Medicaid Services, "Regulations & Guidelines, Enforcement," last modified 04/02/2013. http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/Enforcement/index.html

6 United States Department of Justice, "Federal Register/ Vol. 75, No. 56 / Wednesday, March 24, 2010 / Rules and Regulations. http://www.gpo.gov/fdsys/pkg/FR-2010-03-24/pdf/2010-5816.pdf

7 31 U.S.C. §§ 3729 – 3733.

8 Social Security Act § 1128A, 42 U.S.C. § 1320a-8.

9 Social Security Act § 1128B(b), 42 U.S.C. § 1320a-7b.

10 Omnibus Reconciliation Act of 1989, Pub. L. No. 101-234, 103 Stat. 2106 (1989).

11 *See* 18 U.S.C. 1387.

12 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) ("HIPAA").

13 42 U.S.C. §§ 17931–39.

14 States also have analog laws protecting personal information ("PII") which vary as to scope and breadth.

15 U.S. Department of Health & Human Services, "HIPAA Administrative Simplification Statue and Rules – Health Information Privacy - The Privacy Rule," Accessed April 2014. http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/

16 The U.S. Department of Health and Human Services' ("HHS") definition of "covered entities" includes health plans, health care clearinghouses and healthcare providers or suppliers who electronically transmit any health information in connection with transactions for which the DHHS has adopted standards.

17 DHHS broadly defines "business associate" as a person who: On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or . . . [p]rovides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

18 45 C.F.R. 160, 164.

19 U.S. Department of Health & Human Services, "HIPAA Administrative Simplification Status and Rules – Health Information Privacy – the Minimum Necessary Requirement," December 3, 2002 Revised April 4, 2003. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html

20 U.S. Department of Health & Human Services, "Security Standards: Technical Safeguards," Centers for Medicare & Medicaid Services, Volume 2 / Paper 4, 5/2005: rev. 3.2007. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

21 U.S. Department of Health & Human Services, "HIPAA Administrative Simplification Status and Rules – Health Information Privacy – HHS Releases Request for Information for Accounting of Disclosure Rulemaking," Accessed April 2014. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/accountingrfi.html

22 45 C.F.R. 160.306(c).

23 The breach notification requirements can be found at 45 C.F.R. 164 Subpart D.

24 *CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs,* Department of Health and Human Services, Office of Inspector General January, 2014.

25 The United States Department of Justice, "Abbott Labs to pay $1.5 Billion to Resolve Criminal & Civil Investigations of Off-label Promotion of Depakote," Monday, May 7, 2012. http://www.justice.gov/opa/pr/2012/May/12-civ-585.html