The Anatomy of a Healthcare Data Breach

By Lynn Sessions and Theodore J. Kobus III, Baker & Hostetler LLP

In its 2011 annual report to Congress, the U.S. Department of Health and Human Services (HHS) indicated that from September 23, 2009 to December 31, 2010, over 30,000 healthcare breaches occurred following the implementation of the Health Information Technology for Economic and Clinical Health (HITECH) Act affecting 7.8 million patients.¹ The headlines from 2011 and the first half of 2012 show that healthcare data breaches continue to happen and affect large numbers of patients—three of the largest data breaches in the history of HITECH occurred during the last half of 2011 and impacted nearly 11 million patients.² It is estimated that approximately 60% of healthcare organizations have experienced at least one data breach,³ and these events are proving to be costly to healthcare organizations. HHS has demonstrated a willingness to investigate and hold healthcare organizations accountable for not having their privacy shop in order, including entering into resolution agreements that include civil monetary penalties (CMPs).⁴ Class action attorneys also continue to monitor media reports of large scale data breaches.

Is this what was intended?

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule established for the first time a set of national standards for the protection of certain health information.⁵ A major goal of the Privacy Rule is to ensure that a patient’s health information is properly protected while balancing the need to promote the flow and exchange of health information so that quality healthcare services can be provided.⁶ With the advent of the exchange of electronic protected health information (ePHI) and electronic health records (EHR), additional protections were needed. HITECH, passed in 2009, established those additional protections along with enforcement power to guard against sloppy privacy practices.⁷ The HITECH Act provided for administrative regulations for a national EHR infrastructure including standards and stimulus funding, Medicare/Medicaid incentives for EHR adoption (commonly referred to as “meaningful use” incentives), and notably enhanced HIPAA privacy and security requirements.⁸

The impact of HITECH represents the biggest change to healthcare privacy since the introduction of HIPAA. Key components of HITECH were the introduction of the enforcement provisions, audit allowances, breach notification requirements, and increased fines and penalties. The Office for Civil Rights (OCR) was assigned the investigation and enforcement duties of HITECH violations.⁹ Additional administrative and security requirements were imposed on covered entities, and in 2011, KPMG was awarded the contract to audit healthcare organizations for HIPAA compliance.¹⁰ HITECH defined a healthcare data breach, and along with it, the breach notification requirements. Finally, fines and penalties were increased, as well as enforcement power, to punish covered entities that disregard the new rules and are out of compliance.¹¹
Many states had already enacted state breach notification legislation of their own. Today, over 46 U.S. jurisdictions have breach notification laws that may impact a HIPAA/HITECH breach response. Since most of the state statutes are written in terms that apply when a breach affects "residents" of the states, and certain states have more strict breach notification requirements than HIPAA/HITECH, preemption rules will not apply and the state’s more strict law will govern. The state laws can be a trap for the unwary, particularly for those covered entities that have a national reach. Individual states’ attorneys general have also been trained to enforce HITECH provisions and many are already active in their enforcement of HITECH and their respective state notification laws. Each of the state statutes have their own nuances, with some accelerating notification deadlines and others requiring specific language be placed in the notification letters.

Privacy laws continue to evolve at the state and federal levels with the final HITECH rule hovering for approval since September 2009 and overarching federal privacy legislation being considered by Congress outside of healthcare. The states also continue to refine their privacy and breach statutes, making notification under HITECH a sometimes moving target, when multiple states are involved.

Breaches
Prior to HITECH, there was no federal requirement to notify patients of a healthcare privacy breach. As of September 23, 2009, HITECH mandates for covered entities to notify affected individuals when protected health information (PHI) is breached. HITECH defines a “breach” as “the unauthorized acquisition, access, use or disclosure of PHI, which compromises the security or privacy of the information.” The statute defines “compromises” as that which “poses a significant risk of financial, reputational or other harm” to the individual who is the subject of the incident, which is the risk of harm analysis. HIPAA/HITECH contemplates breaches of PHI contained in electronic and paper format and requires a covered entity to conduct and document the risk of harm analysis. Common breaches include: (1) lost, missing, or stolen laptops or other portable devices; (2) disposal of documents, computers, or other materials; (3) hacking; and (4) third-party mistakes. A covered entity’s management of its business associates is important, including the need for an appropriate business associate agreement requiring the business associate to notify the covered entity of a security incident within, preferably, a short period of time. The business associate rules have not yet been published, so we anxiously await HHS’ intentions regarding HITECH enforcement and compliance in this regard.

HITECH applies to unsecured PHI. A covered entity is required to implement administrative, physical, and technological safeguards to protect its PHI. HITECH allows for a safe harbor for encrypted devices. However, some purveyors of software used by healthcare providers warn against encrypting with reports that encryption may interfere with the functionality of the software in performing the medical or diagnostic study. If encryption is not possible or is cost prohibitive, covered entities must have in place appropriate physical protection (such as badge access only doors or locked cabinets for storing devices) to protect the PHI from access or disclosure. In addition to technological and physical safeguards, covered entities must have administrative safeguards in place in the form of policies and procedures and documentation that the policies and procedures have been implemented. For example, HITECH requires the covered entity perform a risk analysis and respond with a risk management plan to address identified vulnerabilities. The covered entity should not only have a risk analysis policy in place, but also should have the documented risk analysis and the corresponding risk management plan in the event they are requested by OCR.

Notification Requirements
Once a covered entity determines that an incident rises to the level of a breach, the covered entity must determine the manner of notifying the affected patients. HITECH requires notification to each individual whose unsecured PHI has been breached. The notification must be in writing, by first class mail, unless the patient has agreed in advance to receive email communication. It may be by telephone if imminent misuse of the PHI is possible. If the covered entity has insufficient information for 10 or more individuals, substitute notice is required in the form of conspicuous posting on the covered entity’s website for 90 days or conspicuous notice in major print or broadcast media in geographic areas where individuals affected are likely to reside. If there are 500 or more affected persons in a jurisdiction, notice to prominent media outlets is required along with immediate reporting to OCR. The notification must be “without unreasonable delay,” but in no event greater than 60 days after the date of discovery of the breach. The covered entity, however, may be subject to a law enforcement delay should law enforcement request delay of notification so as not to impede their investigation. Note that other factors may complicate notification as well, and HHS has acknowledged that if a written notification will do more harm than good, other methods of notification should be considered.

The notification must include a description of the incident, the date of the breach (if known), the date the covered entity discovered the breach, the type of PHI involved, recommended steps to be taken by the individual to protect themselves from potential harm, a description of the investigation, the types of mitigation or protections implemented by the covered entity to prevent future breaches, and contact information for questions by the affected persons including a toll-free number. Depending on the type of data elements included, state laws could impact the notification content. For example, an electronic breach of PHI that includes social security numbers and occurs in Florida, with patients who reside in Florida, Massachusetts, and Indiana, may likely require an analysis beyond HIPAA/HITECH. Each of these states has different notification requirements, which may be stricter than HITECH. Florida requires notification to its residents within 45 days, and Indiana within 30 days and with notification to
its attorney general. Massachusetts requires attorney general notification and the inclusion of specific language regarding the availability of a security freeze for the consumer to put on their credit file. When certain data elements, such as social security numbers are involved in an electronic breach, the covered entity must look beyond just notification to patients but also to attorneys general and other consumer agencies, OCR, law enforcement, media, and credit reporting agencies. The orchestration of notification on a large-scale breach involves many moving parts.

Response
When a covered entity determines that a breach has occurred, it should activate its breach incident response team. Healthcare organizations are typically well-prepared in responding to a crisis involving codes, emergency management and disaster response, and accreditation surveys. Data breaches should be no different. The breach incident response team should have C-Suite engagement and be comprised of a multidisciplinary team in responding to a privacy incident. This team should include executive leadership who can make decisions, legal/compliance/privacy, information technology, communications, and customer relations. In some instances, security and human resources may also be engaged. The key is for these groups to not meet for the first time when a breach has occurred. Further, decision makers need to be at the table to accelerate and move forward the breach response. A suggested crisis management process includes: (a) daily status report meetings; (b) daily goal setting; (c) assignment of tasks for the team to accomplish; (d) tracking of progress; and (e) decision making. If the team is able to meet prior to the crisis and each member knows their role, the breach management process goes smoother. Setting goals and priorities is a key function of the incident response team; specifically, the priorities should be: (1) end the compromise of security or remedy the risk control deficiencies; (2) restore functioning of the affected systems; (3) determine the root cause of the incident and mitigation and protection to be utilized; (4) evaluate any notice obligations (federal, state, and contractual); (5) outreach to key customer and business partners; (6) prepare media and internal communications; and (7) issue notification. Once these priorities are accomplished, the team should continue to meet regularly to determine the customer, media, and reputational impact to the organization until the crisis has passed. In large-scale breaches, the crisis may truly begin once the patients and media are notified. It is important that the incident response team remains engaged to respond to the issues that arise.

Costs
Ponemon Institute reported that the costs associated with healthcare data breaches remains high. In 2011, Ponemon reported that the total organizational costs for a data breach were $5.5 million with healthcare averaging $240 per each record. A healthcare record is a gold mine of information that criminals may use for a multitude of activities including identity theft, credit fraud, medical identity theft, or tax fraud. Covered entities may incur costs for forensic investigations; printing and mailing of notification letters; credit monitoring, call center, public relations, and crisis management professionals; and legal fees. Each of these engagements may assist the covered entity in mitigating its risk to ultimate regulatory exposure. For example, a forensic investigation may be able to determine whether a computer file had been accessed following the date of a theft or may help narrow an employee’s unauthorized access to patients’ information. In each of these examples, based on the forensics results, a covered entity may notify fewer individuals thereby lowering its overall costs and providing objective evidence in support of the covered entity’s risk of harm analysis. In large-scale breaches, the cost of printing, the hassle of accurately stuffing envelopes, and the postage expense is not inconsequential. These expenses combined with credit monitoring costs often represent the largest expenses in a large-scale breach. For breaches involving social security numbers or financial information, credit monitoring is recommended. Further, many healthcare organizations have internal call centers that may be able to absorb an increased volume of calls and those questions arising from the breach, but many opt for the use of an external call center to manage the calls. One of the most important partners in a large-scale data breach is a crisis management firm that can assist with overall messaging for internal and external communications, train spokespersons for interviews, and manage the media response and media monitoring. These firms specialize in crisis communication management and represent a line of defense for any reputational harm to the healthcare entity. Finally, covered entities should strongly consider hiring experienced and knowledgeable healthcare privacy and data breach attorneys to direct the navigation of HIPAA/HITECH, the various state notification and regulatory requirements, and orchestrate the notification process.

Post-Breach
In the period immediately following notification, the healthcare organization typically spends its time responding to media and affected individuals. In breaches involving greater than 500 people in a jurisdiction, media notification is required. Hospitals and healthcare providers are regarded as trusted members in most communities and when a breach occurs that trust may be affected. Healthcare data breaches are newsworthy stories, and often in addition to the required press release, the media continues with follow-up stories particularly where employees involved in criminal activity are at issue or hundreds of thousands of individuals are affected. While the organization prepares for and responds to the media, patients begin calling the call center with questions regarding their information and the effect of the breach. Each of these may fuel the other and highlights the continued need for incident response team communication and engagement.

After the immediate crisis, the covered entity can expect an OCR investigation. This investigation is designed to determine if the covered entity was in compliance with HIPAA/HITECH and how the breach occurred. The OCR may take several months with several exchanges of information before
reaching a conclusion. This investigation provides the OCR with the information it needs to assess fines and penalties against the covered entity. The covered entity's documentation of its privacy and security rule compliance is critical, as is its compliance with the breach notification rules. Other accreditation and regulatory agencies, such as The Joint Commission, state departments of health, or state attorneys general, may also request information. Additionally, class action plaintiffs’ attorneys, particularly in states where nominal damages are awardable, continue to bring causes of action for disclosure of PHI or challenge the precedent that HIPAA does not give rise to a private cause of action. Most recently, the Office of Inspector General (OIG) announced audits of the use of portable electronic devices of healthcare organizations. While these audits are on the OIG’s 2012 work plan, OIG may be targeting some healthcare organizations that reported breaches involving portable electronic devices.

Protection and Prevention
Covered entities need to remain vigilant and put in place all feasible protections to ward off breaches, regulatory violations, and third party claims. First, the covered entity should ensure it has met the administrative requirements under HIPAA/HITECH with appropriate policies and procedures in place, a designated privacy officer, and implementation of a risk analysis and risk management plan. Next, the organization should put in place all reasonable technical and physical safeguards to maximize compliance under HITECH. Specifically, because of the encryption safe harbor, encryption of all devices, and especially portable devices, should be considered where it is not cost prohibitive. If encryption is not feasible, physical safeguards should be implemented to protect PHI and ePHI. Education and training of all staff to increase organizational awareness of the consequences of the disclosure of PHI is important. The organization can accomplish this through annual required training, regular employee communication, or focused educational sessions, as appropriate. Information technology audits for the organization to assess vulnerabilities and compliance with HITECH should be included as part of an internal audit annual work plan to strengthen protections in a healthcare organization. Organizations should also consider cyberliability insurance or alternative risk financing for an additional layer of protection against healthcare data breaches. These insurance policies may cover a myriad of services and expenses including legal fees, breach notification expenses, and crisis management costs. Some insurers also include risk management services as part of their policies.

Emerging Issues
As healthcare information becomes more electronic and more mobile, this area of health law will continue to evolve. Federal and state statutes are being refined providing additional protections to affected individuals. EHRs, health information exchanges, and patient portals—all which are advocated by meaningful use—may expose additional vulnerabilities as healthcare organizations implement patient- and provider-friendly systems. Wireless and mobile devices give rise to easy losses and possible disclosure, especially when lacking encryption or other security. Access to large volumes of personal information has caused healthcare organizations to be the targets of criminal activity with the recruitment of healthcare employees to steal data. Cloud computing and offshoring of data present additional challenges in securing PHI in the cloud and in foreign jurisdictions. One thing is certain: privacy and protection of PHI will continue to be a focus and concern for healthcare organizations, their patients, and the federal and state agencies that regulate the industry.

About the Authors
Lynn Sessions (lsessions@bakerlaw.com) is a healthcare attorney with Baker Hostetler in Houston, TX. She is a member of the firm’s Healthcare Industry Team and the Privacy, Security and Social Media Team. Ms. Sessions focuses her practice on providing legal services to healthcare industry clients, including hospitals, integrated delivery systems, physicians and physician group practices, nurses, and academic medical centers. Using her prior in-house experience at Texas Children’s Hospital, Ms. Sessions represents and provides legal counsel to clients on a variety of privacy and data security matters from an in-house counsel and client perspective. She has provided legal counsel to clients where multiple parties in various states were involved in high stake data privacy security breaches.
Theodore J. Kobus III (tkobus@bakerlaw.com) is National Co-Leader of Baker Hostetler’s Privacy, Security and Social Media Team, based in New York, NY. Mr. Kobus focuses his practice in the areas of privacy, data breaches, social media and intellectual property. He advises clients regarding data security and privacy risk management, breaches, response strategies, litigation and regulatory actions affecting organizations. Mr. Kobus has counseled clients involved in significant breaches implicating state and federal laws, international laws, and other regulations and requirements, such as the HITECH Act, the Massachusetts Data Privacy Law, California privacy laws, and many other state laws. He has handled over 250 breaches in various industry segments that include healthcare, education, banking, technology service providers, hospitality and retail.

Endnotes

Thanks go to the leadership of AHLA’s In-House Counsel Practice Group for sponsoring this feature: Richard G. Korman, Senior Vice President/General Counsel, Avera, Sioux Falls, SD (Chair); Terri A. DeSio, Texas Health Resources, Arlington, TX (Vice Chair – Strategic Activities); Susan Feigin Harris, Baker & Hostetler LLP, Houston, TX (Vice Chair – Membership); Kimberly K. Otte, Mayo Clinic, Rochester, MN (Vice Chair – Educational Programs); Davis W. Turner, Vice President & Assistant General Counsel, Vanguard Health Systems Inc., Nashville, TN (Vice Chair – Research & Website); Charles R. Whipple, General Counsel, Hallmark Health System, Melrose, MA (Vice Chair – Publications).

Follow the In-House Counsel Practice Group on Twitter @AHLA_In_House

Don’t miss AHLA’s In-House Counsel Program and In-House Counsel Practice Group Luncheon on June 24, 2012 in Chicago, IL. For more information, see page 18 or go to www.healthlawyers.org/annual12.