HIPAA Privacy/Security Rules: Where We've Been and Where We Are Going

Updates from the HITECH Act to Dramatically Impact HIPAA Privacy/Security

*Neville M. Bilimoria, Esq.**

When HIPAA was passed, many applauded the portability aspects of HIPAA that allowed for continuing healthcare coverage for individuals who lost their jobs and attendant healthcare insurance. But few back in 1996 anticipated the dramatic impact that HIPAA would have later on the privacy and security of health information in the United States. This article discusses not only the history of HIPAA Privacy and Security Rules, but also dramatic new privacy and security laws under the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed February 17, 2009, that will affect how physicians and other healthcare providers comply with the many and sometimes onerous requirements of the HIPAA Privacy and Security Rules.

HIPAA HISTORY

Subtitle F of HIPAA concerned "administrative simplification" that required Congress in future years to establish standards and requirements for the electronic transmission of health information and the privacy and security of that information before 1999. Within the HIPAA legislation itself, Congress imposed a deadline on itself to provide for health privacy and security under the administrative simplification aspects of HIPAA. But because Congress did not act in this regard in a timely manner, HIPAA had a fallback whereby its authority to create such rules would eventually expire and transfer to the United States Department of Health and Human Services (HHS). In 1999, HHS was suddenly charged through HIPAA with creating broad federal rules to protect health information privacy and security. Therefore, on December 28, 2000, HHS issued proposed rules for the privacy of healthcare in America, referred to as the HIPAA Privacy Rules.

The new proposed HIPAA Privacy Rules were initially met with heated resistance from the healthcare provider community, with the American Hospital Association claiming that the HIPAA Privacy Rules would be burdensome and would increase cost and paperwork in the form of consents and other types of authorizations and compliance that the proposed Privacy Rules envisioned. Not to be outdone, the American Association of Physicians and Surgeons filed a federal lawsuit in Houston, Texas, to block the implementation of the Privacy Rules for the same reasons, indicating that it would cause much undue hardship on physicians and physician practices, and impose greater costs with no real benefits. Eventually, after significant revision to the proposed Privacy Rules, the lawsuits and lobbying efforts stopped, and focus turned toward reluctant compliance with the new HIPAA Privacy Rules. Compromises were made with HHS and revisions were made to the Privacy Rules, and a new compliance date was set for April 14, 2003. The Security Rules went into effect on April 21, 2005.

ENFORCEMENT

HHS designated the Office for Civil Rights (OCR) as the enforcer of the HIPAA Privacy Rules, and OCR quickly indicated that it would emphasize assisting providers to move toward voluntary compliance with the Privacy Rules instead of imposing penalties for violations initially. Within one year of the enactment, there were over 4755 complaints filed with OCR for privacy violations. A year later, over 10,785 complaints were filed, and Figures 1 and 2 show the number of enforcement complaints and investigations conducted by the OCR through February 2009.

HHS noted that the most common complaints were alleged impermissible use or disclosure of patient information and failure to provide individuals with access to their medical records. Private healthcare practices, such as physician practices, had the most complaints, followed by hospitals, pharmacies, outpatient centers, and then group health plans. Other than certain high-profile cases, HIPAA privacy enforcement was relatively low-key over the first six years of the HIPAA Privacy Rules.

*Partner in the Chicago office of Duane Morris LLP; Member of the Health Law Practice Group; and Chair of the Physician Services Group nationally; phone: 312-499-6758; e-mail: nmbilimoria@duanemorris.com.

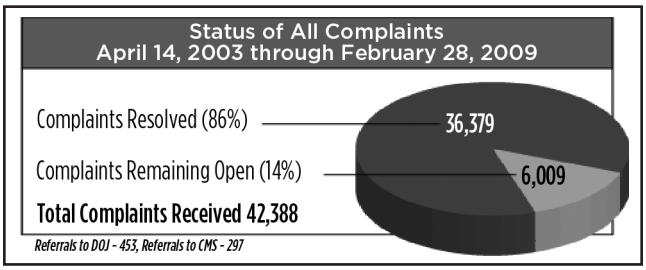

Figure 1. Status of all complaints. CMS, Centers for Medicare & Medicaid Services; DOJ, Department of Justice.

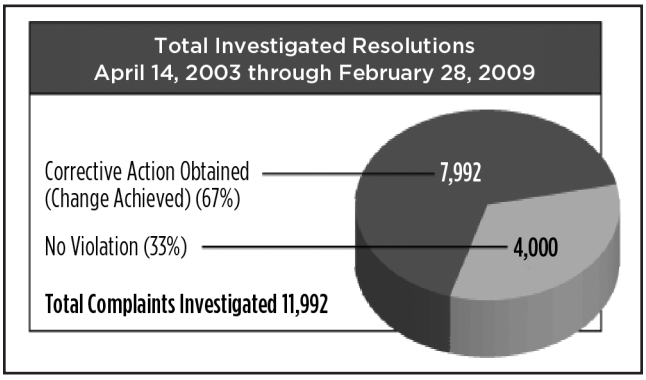

Figure 2. Total investigated resolutions.

Eventually, as time has gone by, most healthcare providers in the United States have fully embraced the HIPAA Privacy and Security Rules, and generally HIPAA has been touted as a key law for the protection of patients everywhere. The initial reluctance to comply with HIPAA Privacy and Security Rules has now been replaced with a desire to become fully HIPAA-compliant, even as a public relations tool to foster goodwill with patients across the United States.

As new healthcare providers enter the workforce, many HIPAA compliance programs have gathered dust or are not adhered to as strongly as before, especially in light of the relatively mild enforcement to date of the HIPAA Privacy and Security Rules. However, that seems to be changing with the Obama Administration, and more and more providers are becoming aware that HIPAA privacy and security compliance is more important than ever, especially in light of the changes forthcoming through the HITECH Act and the proliferation of electronic health records (EHRs).

TIPS FOR ONGOING HIPAA PRIVACY RULE COMPLIANCE

During the initial stages of HIPAA Privacy Rule implementation, there was a considerable amount of confusion regarding what the HIPAA Privacy Rules provide and what they require given the length and breadth of the regulations themselves. Soon hospitals and other providers began to hone and fine-tune their HIPAA compliance programs to the letter of the Privacy Rules. However, recently—and it seems to happen in waves—new or unsophisticated healthcare providers have been falling into the many traps of "HIPAA-mania," only to find themselves being noncompliant with the true requirements of the HIPAA Privacy Rules. Below are some common and important tips to avoid HIPAA Privacy Rule overkill in your HIPAA compliance program.

Authorization Overkill

Many providers have requested HIPAA authorizations under the guise of the Privacy Rule, claiming that authorizations are required under the Privacy Rule when in reality they are not required. It is important to remember that the main point of authorizations is to ensure that covered entities obtain patient approval when protected health information (PHI) is not being sought for the day-to-day business of healthcare. The following are some examples of when a HIPAA authorization is *not* needed:

1. *Treatment, payment, and healthcare operations*:
   - Do not worry about needing an authorization to disclose a patient's PHI to another provider for treatment.
   - You do not need an authorization when releasing PHI to payers, ambulance companies, or insurance companies for payment.
2. *HIPAA-accepted uses and disclosures under Section 164.512:* You do not need an authorization if a disclosure is required for the following reasons:
   - Required by law;
   - Public health activities;
   - Victims of abuse, neglect, or domestic violence;
   - Health oversight activities (agency surveys or enforcement);
   - Judicial or administrative proceedings (with certain restrictions);
   - Law enforcement purposes;
   - Decedents, funeral directors, etc.;
   - Cadaveric organ, eye, or tissue donation;
   - Research purposes;
   - To avert serious threat to health or safety;
   - Specialized government function; and
   - Worker's compensation laws.
3. *Professional judgment*: If the person seeking PHI is not the patient himself or herself, but is involved in the patient's care, the covered entity may reveal PHI to the person without an authorization, as long as the patient has not objected to doing so. As long as a covered entity makes reasonable attempts to verify the person's identity and the involvement of the person in the patient's care, the HIPAA Privacy Rules allow for professional judgment in those instances and do not require an authorization. This even works for situations over the phone.

4. *Minors' rights*: Parents and legal guardians usually do not need authorizations to obtain their minor children's PHI. However, state law may require authorizations if the minor is emancipated or when state law allows minors to be in charge of their own treatment (e.g., family planning, mental health, HIV, sexually transmitted diseases).
5. *Emergency situations*: When a patient is incapacitated and an emergency warrants patient PHI disclosure, professional judgment may be used without the need to obtain an authorization beforehand. An authorization will have to be obtained afterwards if it is required under the HIPAA Privacy Rules once the emergency situation has subsided.

HIPAA Logs

HIPAA also requires a number of logs to be maintained by covered entities to comply with the HIPAA requirements. Here are examples of three key logs that are required to be maintained by covered entities:

1. *Complaint logs*: A covered entity must document all complaints received and their disposition, if any. This may include investigations of HIPAA Privacy and Security breaches and steps taken to mitigate any wrongfully disclosed PHI through the covered entity's HIPAA compliance plan.
2. *Sanction logs*: A covered entity must have and apply for sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the HIPAA Privacy and Security Rules. The covered entity must document all sanctions that are applied, if any, to employees who fail to comply.
3. *Accounting logs*: A covered entity must maintain descriptions of its uses and disclosures for purposes of the accounting requirements under the HIPAA Privacy Rules. These accounting logs may be used to respond to patients who inquire about the uses and disclosures of their PHI.

RECENT HIGH-PROFILE CASES

Recently, HIPAA Privacy and Security Rules have gained national attention through severe fines and penalties assessed by HHS against certain healthcare providers. Two of these cases involve Providence Health System and CVS Caremark Corp.

On July 15, 2008, HHS entered into a Resolution Agreement with Providence Health & Services, Providence Health System-Oregon, and Providence Hospice and Home Care, all related nonprofits based in Washington and Oregon (collectively, "Providence"). The agreement resulted from an HHS investigation of five incidents in late 2005 and early 2006 in which Providence staff members, in violation of applicable security policies, had taken off premises laptops, tapes, and disks that contained electronic protected health information (ePHI). The media and laptops were subsequently lost or stolen. There was no indication in the documents that the ePHI at issue was improperly used by the persons who stole the laptops, tapes, and disks, or any other party, or whether the ePHI was ever recovered.

Under the Corrective Action Plan appended to its Resolution Agreement, Providence is subject to tough compliance terms that include revised policies and procedures, re-training for all workers, and increased self-auditing. In addition, the agreement imposed outside monitoring and regular reporting requirements. If HHS is not satisfied with Providence's intensified compliance activities, Providence is potentially subject to fines in addition to the original $100,000.

More recently, on February 18, 2009, CVS Caremark Corp. agreed to pay $2.25 million to settle a federal investigation into allegations that it violated HIPAA privacy regulations when pharmacy employees threw items such as pill bottles with patient information into the trash.

The settlement followed a joint investigation by the HHS and the Federal Trade Commission after media reports in 2006 that workers at CVS pharmacies were improperly disposing of sensitive patient and employee data.

Employees allegedly tossed pill bottles with labels containing patient information into open dumpsters, along with medication instruction sheets, pharmacy order information, employment applications, payroll data, and credit card and insurance card information.

In addition to paying HHS $2.25 million, the company's more than 6000 retail pharmacies must establish and implement policies and procedures for disposing of PHI, implement a training program, conduct internal monitoring, and hire an outside assessor to evaluate compliance for three years.

WHERE HIPAA PRIVACY AND SECURITY RULES ARE HEADED

On February 17, 2009, the American Recovery and Reinvestment Act of 2009 was passed, containing a set of provisions, known as the HITECH Act, that advance the use of technology in healthcare, principally by encouraging hospitals and physicians to adopt an EHR system before the end of 2015. Under the HITECH Act, HIPAA Privacy and Security Rules must be amended in a way that will affect physicians and their practices. Below are some of the key changes to HIPAA mandated by the HITECH Act.

- **Business Associates on the Hook:** Under HIPAA, business associates were subject to contractual breach *only* if they failed to comply with Privacy and Security Rules. Under the HITECH Act, covered entities will now include "business associates" who will be directly subject to HIPAA's privacy and security requirements, including administrative, physical, and technical

safeguard requirements (such as the need to develop and implement comprehensive written security policies and procedures with respect to the protected health information), as well as its criminal and civil fines and penalties. This will require business associate agreements to be reworked or amended.

- **Clarification of HIO (Health Information Organization):** Also, the HITECH Act maintains that organizations that provide data transmission of PHI to covered entities or their business associates, such as health information exchange organizations, regional health information organizations, or vendors that contract with a covered entity to allow that covered entity to offer a personal health record to patients as part of its EHR, are considered business associates and must have a business associate agreement with such covered entities.
- **Breach Notification:** Under the HITECH Act, there are new breach notification requirements for all covered entities requiring the covered entities to report most security breaches directly to individuals. Large security breaches must be reported to HHS and prominent media outlets. On September 23, 2009, HHS created new Subpart D: "Notification in the Case of Breach of Unsecured Protected Health Information" within the HIPAA Privacy Rule. Under Subpart D, these new amendments took effect September 23, 2009, with enforcement to occur on or after February 23, 2010.
- **Minimum Necessary:** Under the HITECH Act, covered entities must, when otherwise permitted, disclose only the "minimum necessary" to accomplish the intended purpose for such disclosure. There will be new guidance issued governing what constitutes "minimum necessary" for purposes of disclosures under the privacy rule within 18 months after the date of enactment of the HITECH Act (August 17, 2010).
- **Accounting:** Currently, patients can request an accounting of PHI disclosures dating back six years from the request, and HIPAA doesn't currently require disclosures for treatment, payment, and healthcare operations to be included in the list. Under the HITECH Act, individuals may request an accounting of the disclosures of their ePHI over the preceding three years, but the Act requires covered entities to include treatment, payment, and healthcare operations disclosures.
- **Miscellaneous Provisions:**
  - — Under the HITECH Act, individuals may request that their PHI not be disclosed to their health plan if the individuals pay for their medical care in full.
  - — Under the HITECH Act, the definition of "health care operations" will be reviewed by the Secretary of HHS by August 17, 2010, and narrowed or clarified by regulations.
  - — Under the HITECH Act, the HIPAA Privacy Rule is amended to limit when a covered entity may disclose PHI as part of a healthcare operation if it receives or has received a direct or indirect payment in exchange for making such communication, except in specified circumstances.
  - — Under the HITECH Act, the sale of PHI by a covered entity or a business associate is prohibited without patient authorization except in certain detailed, specified circumstances.

CONCLUSION

In all, healthcare providers have come a long way in protecting PHI, and it is likely through the advent of EHRs and their increased promotion under the HITECH Act that healthcare providers will have to continue to be diligent in enforcing their HIPAA compliance plans and updating them to meet the requirements set forth by the new HITECH Act. While initial compliance with the new requirements of the HITECH Act will also be met with some reluctance, as the initial HIPAA Privacy and Security Rules were met with reluctance back in 2003, eventually healthcare providers will realize that patients value their privacy, and these efforts to maintain those privacy protocols through HIPAA Privacy and Security Rules actually promote the sound delivery of healthcare amidst ongoing updates in technology. As we move toward stricter requirements for healthcare privacy in the United States, we can expect this trend to continue as long as patients value their privacy, a commodity that does not seem to lose value in the United States. ■