HIPAA Enforcement: WHAT WE CAN LEARN

BY PATRICIA KROKEN, FACMPE, FRBMA, CRA

The Office for Civil Rights (OCR) recently announced that Blue Cross Blue Shield of Tennessee (BCBST) was fined $1.5 million following an investigation regarding a reported breach under the Health Information Technology for Economic and Clinical Health (HITECH) Act. And in January 2012, the OCR released a report on its enforcement activities under the Health Insurance Portability and Accountability Act (HIPAA), although financial penalties were not referenced in that document.

Was it only 10 years ago that we were struggling to understand how HIPAA would impact our daily operations in radiology as we developed our compliance plans? The regulations were often vague and there were innumerable questions of "What does HIPAA say about_____?" that remained unanswered, since the regulations did not provide detail regarding the government's specific expectations—only the general expectation that we would comply. We also knew the regulations allowed for "scalability" so that the small medical practice would not be expected to have as robust a security system as the large healthcare entity.

As with Medicare Fraud and Abuse compliance, it was evident we would need experience and enforcement results to know what "HIPAA says about_____." That information, and the ability to adjust our compliance activities, is now beginning to emerge.

HIPAA Privacy and Security Rules—Joined by HITECH

The HIPAA Privacy Rule became effective April 1, 2003 and it addresses all forms of communication containing Protected Health Information (PHI), whether on paper, exchanged electronically, or even verbal. Healthcare entities are required to have a posted "Notice of Privacy Practices" outlining permitted "uses and disclosures" under the regulations. Over the years we have dealt with misinterpretation of the regulations both by patients and other healthcare entities, along with incidents reported here and there.

The OCR report states that since the compliance date in 2003, the department has investigated 67,554 privacy complaints. OCR resolved 15,358 of the cases by requiring changes in privacy practices (usually policies and procedures) and other corrective actions by the covered entities.

In 8,026 cases OCR found that no violation had occurred and that the remaining 34,014 cases completed were not considered eligible under the Privacy Rule. In other words, the violation occurred prior to the compliance date, involved an organization that was not classified as a "covered entity" required to comply with HIPAA, was not pursued by the person filing it, or did not violate the rule (such as times when the entity appropriately disclosed information as permitted under the rule).

Among the interesting factoids in the OCR report was a classification of the compliance issues in order of frequency. They are as follows:

- Impermissible uses and disclosures of Protected Health Information
- Lack of safeguards to protect PHI
- Lack of patient access to PHI
- Uses or disclosures in excess of the Minimum Necessary PHI
- Complaints to the covered entity

Covered entities required to take corrective action to achieve voluntary compliance following a HIPAA violation were also listed in order of frequency and included the following:

- Private practices
- General hospitals
- Outpatient facilities
- Health plans
- Pharmacies

So while the large company/large penalty cases grab the headlines, based on history to date the private practice is statistically more likely to face an enforcement activity.

Before detailing some of the examples provided in the OCR report, it is also a good idea to see how violations under the Security Rule compare. The compliance date for the Security Rule was April 20, 2005 and authority for enforcement was transferred to the OCR in 2009. Since that time, OCR reported approximately 521 complaints alleging a violation of the rule and as of Jan. 31, 2011 they reported 258 open complaints and reviews.

The Health Information Technology for Economic and Clinical Health (HITECH) Act was included in the American Recovery and Reinvestment Act of 2009 (Stimulus Program) and signed into law on Feb. 17, 2009. While the stated goal of the regulations was to promote the adoption and meaningful use of health information technology, one section of the HITECH Act addresses privacy and security concerns associated with the electronic transmission of health information. The new rules included reporting requirements in the event that protected health information was compromised and several provisions that strengthened the civil and criminal enforcement of the HIPAA rules, including an increase in the minimum penalty for each violation.

Examples of HIPAA/HITECH Violations

One of the most frightening violations occurred in a radiology practice—frightening because it involved processing inaccurate billing information received from a hospital and could happen to virtually any hospital-based practice. The group submitted a workers' compensation claim to the patient's employer and included the radiology report. However, the patient was not covered by workers' comp for this condition and did not identify workers' comp as the guarantor for payment. The OCR reported the practice's corrective actions included:

1. An apology to the patient
2. Sanctions of the employee responsible for the incident
3. Training staff on coding and appropriate claims submission procedures
4. Revision of policies and procedures to require a request from work comp carriers before submitting a report with a claim

The reality of this situation is that the sanctioned employee was no doubt conducting business as usual, since most workers' comp carriers require submission of a radiology report. The real question is whether practices should instead change their claims submission policies requiring a denial and request for report as standard operating procedure. Each group will have to make a determination regarding risks related to inappropriately filing versus cash flow delays and additional administrative processes if a denial/request for report must occur first. (Even then, it is possible the information would be sent to the employer if the patient did not respond quickly to the initial submission.) ***The violation: Impermissible uses and disclosures.***

A hospital-based radiology practice usually has access to hospital information technology in order to resolve billing-related issues. The temptation to "peek" at the records of a friend, family member, or celebrity can result in a HIPAA violation. In one of the OCR examples given, a nurse practitioner with privileges at a multi-hospital healthcare system looked up the medical records of her ex-husband. The entity took aggressive steps both to resolve this matter to the OCR's satisfaction and to prevent a recurrence, including:

1. Termination of the nurse practitioner's access to the electronic records system
2. Reporting her conduct to her licensing authority

3. Remedial Privacy Rule training

The violation: impermissible use of PHI.

In another example, a private practice accidentally faxed medical records to the patient's employer rather than to his/her new healthcare provider. Unfortunately the records disclosed the patient's HIV status. Corrective actions included:

1. An apology to the patient from both the physician and staff member responsible for faxing the information
2. Written disciplinary warning to the employee
3. Revision of the fax cover page to emphasize information represented a confidential communication for the intended recipient
4. Training for all employees regarding the incident, including proper faxing procedures

The violation: safeguards.

In another private practice example, the group relied on state regulations stating that a covered entity can provide a summary of the patient's records rather than the complete record. The OCR provided "technical assistance" in this instance, advising the group that a summary can be provided only if the patient agrees in advance. Corrective actions included requiring the group to change its policy and forwarding the complete record as requested.

The Violation: Patient access to PHI (for minor child).

The Blue Cross Blue Shield of Tennessee (BCBST) case also has some chilling implications, since it would seem that appropriate measures had been put in place to secure the equipment in question. The $1.5 million paid was classified as a settlement, did not represent an admission of liability, and was established to "avoid the burden and additional expense of investigation and litigation…."

BCBST had moved to a new building and all staff vacated the old site by the end of June 2009. However, they maintained a secured network data closet in the old location where the property manager also agreed to provide security services. Servers in the data closet were scheduled to be moved to the new building in November 2009. Physical security measures included a biometric and keycard scan security with a magnetic lock and an additional door with a keyed lock.

Early in October 2009, employees discovered that computer equipment, including 57 hard drives containing encoded electronic data, had been stolen. Data on the hard drives included more than 300,000 video recordings and more than one million audio recordings of customer service calls. The stored data had to be manually and individually reviewed in order to obtain access to the PHI, which included member names, identification numbers, diagnosis codes, dates of birth, and Social Security numbers. BCBST confirmed that the hard drives contained PHI for 1,023,209 individuals and followed the requirements for reporting a security breach as mandated by the HITECH regulations.

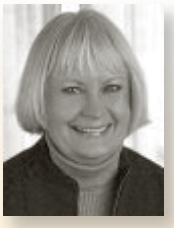
The problem began when BCBST received an alert on a Friday showing that the server at the facility was unresponsive but did not respond or investigate the situation until Monday. The alert did not contain any indication of theft and loss of the server did not appear to otherwise adversely impact operations.

In addition to the financial settlement, BCBST must comply with a Corrective Action Plan (CAP) that includes the following provisions:

1. Submission of privacy and security policies and procedures for the approval of Health and Human Services (HHS), with any revisions as necessary following HHS review
2. Documentation that procedures were implemented and employees trained
3. Certification from individual employees stating they have read, understand, and consent to abide by the policies and procedures
4. Content of the P&P must include:
    a. Completion of a risk assessment
    b. Conduct of a risk management plan implementing appropriate security measures
    c. Appropriate facility and access controls
    d. Physical safeguards governing the storage of electronic records containing PHI
5. Process to report violations (reportable events)
6. Unannounced site visits as part of "monitor reviews" to inspect facilities housing portable devices, random employee interviews, and inspections of random samples of portable devices

The most sobering aspect of reviewing any of these violations is that they could happen in virtually any radiology practice or billing company—and several of them have. In some instances, the corrective actions taken provide insight into steps that might be proactively taken to avoid similar situations. In others, there is only an "after the fact" admonition, although guidelines for recommended actions are provided in the event a violation occurs.

More examples can be found at: **http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/casebyentity.html#2privatepractice**



PATRICIA KROKEN, FACMPE, CRA, FRBMA is a principal in Healthcare Resource Providers, a radiology business consulting firm. She is a regular contributor to industry publications and a frequent speaker on topics related to radiology practice management and HIPAA. *Patricia can be reached at Healthcare Resource Providers, LLC, PO Box 90190, Albuquerque, NM 87199; 505.856.6128; pkroken@comcast.net.*