ADAM MICHELMAN

An Update on What Is Being Done to Keep Protected Health Information Secure

Adam Michelman specializes in legal and regulatory analysis at Strategic Management Services, LLC, a health care consulting firm that provides specialized HIPAA compliance advisory services. For more information, see www.strategicm.com or call him directly at 703/683-9600.

Recent High-Profile Privacy Breaches Bring HIPAA Issues into the Public Eye

Health Insurance Portability and Accountability Act (HIPAA) violations and enforcement are not exactly what one expects to see when they open up a celebrity gossip magazine or the sports section of the newspaper. A few recent high-profile violations, however, have brought HIPAA issues into the public eye.

A California medical center fired 13 employees for improperly accessing the confidential medical records of pop star Britney Spears. In a separate incident, the same medical center disciplined an employee for snooping in actress Farrah Fawcett's medical records. Just last month, 20 hospital workers were fired for accessing medical records of NFL player Richard Collier after he was the victim of a shooting.

These incidents brought HIPAA to the attention of the mainstream media, but these were not the only major cases since HIPAA's privacy rule became effective in 2003. At hospitals and government agencies, stolen laptops, programming errors, and even disgruntled employees have caused the exposure of the health records of millions of individuals. This is where the real story lies; look past the glamour of the newsworthy patients, and the issue of whether medical records are being kept safe is very real.

There appears to be more questions arising from media accounts than answers in the enforcement of HIPAA. Has the Centers for Medicare & Medicaid Services (CMS) used its disciplinary authority with enough frequency? Where does the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforcement effort fit into the equation? Can privacy breaches like these really only be happening to celebrities? Are they the only ones that matter? What about the rest of us and

our families? If a hospital is not under investigation by CMS, does that mean they are truly keeping data safe?

These recent headlines, combined with a new report on CMS's policy of HIPAA oversight by the Office of Inspector General (OIG), call into question whether CMS is preventing the occurrence of HIPAA violations with a proper level of veracity. More importantly, they suggest that hospitals are failing to keep protected health information secure.

When an individual, celebrity or otherwise, has concerns regarding the privacy practices of a health plan or covered provider, these complaints can be made directly to the covered provider or health plan or to OCR. OCR is charged with the authority to investigate complaints and enforce HIPAA privacy regulations. On October 23, 2003, however, HHS published a ruling in the *Federal Register* that delegated certain authorities to CMS regarding security provisions implemented in the enforcement of HIPAA, including interpreting, implementing, and enforcing the HIPAA security rule provisions, as well as conducting compliance reviews and investigating and resolving complaints of HIPAA security rule noncompliance. Finally, it was charged with imposing civil monetary penalties for a covered entity's failure to comply with HIPAA security rule provisions.

Although enforcement of the security rules has been delegated to CMS, the HIPAA privacy rules remain the domain of the OCR, and considerable overlap remains between them. For example, paper-based health information such as medical charts and sign-in sheets are governed by the privacy rule while electronic transmissions of information between covered entities falls under the security rule. It is not difficult to imagine instances in which violations of both rules are occurring. In these situations, CMS and OCR jointly investigate the cases. OCR tends to receive a much greater number of complaints, although in many instances it leads to the forwarding of cases to CMS for investigation into security rules violations.

OCR has long been the subject of critics who suggest that its enforcement strategy has not been aggressive enough to truly get the attention of the health care community. With its recent delegation to CMS, the new question being asked is how effective CMS has been in its new role as enforcer of the HIPAA security rule provisions.

Evidence suggests that CMS, like the OCR, may not be meeting expectations. In a recent report on CMS's policy of HIPAA oversight, the OIG found that CMS had taken limited actions to ensure that covered entities adequately implemented the HIPAA security rule. Despite being authorized by federal regulations to take a more proactive approach involving compliance reviews, CMS "relied on complaints to identify any noncompliant entities that it might investigate." Based on this finding, the OIG indicated that the reliance on incoming complaints alone is an ineffective system for identifying noncompliant covered entities.

Ongoing OIG audits of hospitals nationwide indicate that under the current CMS enforcement system, celebrities are not the only ones whose confidential information is at risk. OIG found numerous vulnerabilities in the controls currently in place at hospitals to protect electronic protected health information (ePHI). The OIG also noted that CMS received "very few" complaints regarding potential HIPAA violations and that many of the vulnerabilities it identified would not have been flagged by HIPAA security rule complaints.

As of October 31, 2005, CMS received only 413 potential security rule complaints out of more than 16,000 total HIPAA complaints. Given these facts, the OIG stressed the importance of CMS initializing its authority to take a proactive approach to evaluating compliance. In addition, although the OIG noted that reliance on complaints alone was ineffective for identifying noncompliant entities, the OIG further noted

that the CMS process for receiving, categorizing, tracking, and resolving complaints was an effective one.

"This is a formalized wakeup call for CMS; as an enforcement arm, it will be held accountable to fulfill its duties," said John C. Parmigiani, MS, BES, president of John C. Parmigiani & Associates, LLC, in Ellicott City, Maryland, and former chairperson of the team that created the HIPAA security rule. "But it also says to the health care industry that CMS is going to be coming after you."

CMS, in its official response, agreed that compliance reviews are a useful enforcement tool. Specifically, CMS officials noted their execution of a contract with PriceWaterhouseCoopers in 2007 that includes performing onsite reviews of certain covered entities. CMS disagrees, however, that enforcement of the HIPAA security rule should be focused solely on compliance reviews of covered entities. CMS considers compliance reviews to be useful as part of a more "comprehensive enforcement strategy that also includes complaint investigation and resolution, outreach, education, and working closely with industry to identify and correct security issues."

As a result, CMS noted that the agency has taken measures "to enable the industry to benefit from the issues identified from an individual case or compliance review" and "heighten the industry's understanding of HIPAA security requirements and the various means by which utilities can comply." CMS began posting case studies based on complaint data on the CMS Web site in 2008. Furthermore, the agency has made additional educational material (such as Frequently Asked Questions, guidance documents, and educational papers) available to covered entities. CMS also noted that it has further expanded its outreach efforts by participating at industry conferences to address HIPAA security issues relevant to covered entities.

The OCR has long been the focus of critics for what is seen as ineffective enforcement of HIPAA violations, but it also seems to be taking the criticism to heart. A joint settlement between OCR and CMS and a health care organization in June 2008 marked the first instance of a covered entity paying a fine since the enactment of the privacy and security rules. "It's fair to say that in the first year or so, we were using education and technical assistance with covered entities to get them into compliance, but it's also true that covered entities should be taking responsibility for compliance now," said Susan D. McAndrew, JD, deputy director of health information policy for the OCR. "Enough time has passed for entities to know what their obligations are, and we have a variety of compliance tools that we are willing to use."

The question remains: Is a plan of comprehensive enforcement the best strategy to protect patient data? "If you just focus on a complaint, and resolving that complaint, that's not enough," said Kate Borten, CISSP, CISM, president of The Marblehead (MA) Group. "The OIG went in and found all these other problems that would never have come to light without a full compliance review." Given the findings of the OIG report and the unfortunate rash of high-profile cases in which patient information was compromised, hospitals can expect to be under stricter scrutiny than ever before when it comes to protecting patient information.

While the next steps by CMS and the OCR might not be known, the onus has always been on the hospital first. Change in some fashion is likely on the horizon, but the best course of action is to avoid an investigation by having a system in place that leaves little to investigate in the first place. All this may be a wake-up call for hospitals to conduct an independent review of their HIPAA privacy and security program and controls.