Crack Down
Proper HIPAA Privacy Controls and Training Could Help Prevent Criminal Liability for Wrongful Access and Disclosure

A recent wave of patient data security breaches by employees of HIPAA-covered entities have led to the government’s growing commitment to more aggressive efforts to identify and criminally prosecute HIPAA violations. Accordingly, in May 2008, a nurse employed by an Arkansas clinic was criminally convicted of wrongfully disclosing individually identifiable health information for personal gain and malicious harm. The nurse pled guilty to allegations stemming from her improper access of private medical information of a patient November 2006, and her subsequent disclosure of the medical information to her husband. Her husband intended to use the information against the patient in an unrelated legal proceeding. In connection with her conviction, the nurse faces criminal penalties under HIPAA, along with a term of supervised release up to three years.

Similarly, in April 2008, a UCLA Medical Center employee was indicted on a felony count of illegally obtaining individually identifiable health information for commercial advantage and faces imprisonment of up to 10 years, if convicted. The employee, who resigned her position as an administrative specialist, allegedly accessed the private medical records of celebrity patients and sold confidential information to a national media outlet.

Since these privacy violations were disclosed, California state legislators have discovered that more than 120 other employees of UCLA Medical Center illegally accessed celebrity medical records and sold confidential information to a national media outlet.

As a result of this ongoing investigation UCLA Medical Menter was cited for deficiencies and is required to submit a plan of correction to the California Department of Health.

HIPAA holds any person who knowingly obtains or discloses any individually identifiable health information relating to a patient criminally liable. The penalties for these violations include a minimum fine of $50,000 and imprisonment up to one year. If the violation was committed with the intent to sell, transfer or use the health information for commercial advantage, personal gain or malicious harm, the penalties include a fine of up to $250,000 and imprisonment of up to 10 years.

While only a handful of HIPAA criminal cases have been prosecuted since the 2005 deadline for compliance with the rule, this recent prosecution may mark a new initiative of heightened government scrutiny and serves as a reminder of the consequences for breaching HIPAA privacy protections.

“What every HIPAA-covered entity needs to realize and reinforce to its employees is that the privacy provisions of HIPAA are serious and have significant consequences if they are violated,” says Jane W. Duke, United States Attorney for the Eastern District of Arkansas. “Long gone are the days when medical employees were able to snoop around the office files for information to share outside the office. We are committed to providing real meaning to HIPAA. We intend to accomplish this through vigorous enforcement of HIPAA’s right-to-privacy protections and swift prosecution of those who violate HIPAA for economic or personal gain or malicious harm.”

Similarly, the California State Senate recently passed a bill that would require healthcare providers to implement safeguards to protect patients’ individually identifiable medical information. If passed, this legislation would create a statewide Office of Health Information Integrity within the California Health and Human Services Agency. The director of this newly established office would be vested with the power to assess fines of up to $250,000 against violators of the patient privacy rules, and make recommenda-
tions on further investigations, discipline and licensing decisions.

The recent prosecutions against an Arkansas nurse and a California administrative specialist may also indicate a trend toward holding individuals, in lieu of or in addition to covered entities, accountable under HIPAA for wrongfully accessing and using patient private information for personal gain. While a 2005 memorandum opinion prepared for the General Counsel of the HHS and the Senior Counsel to the Deputy Attorney General described a narrow scope of liability under the HIPAA criminal provisions, the recent prosecutions against employees of covered entities demonstrate movement toward a more expansive scope.

The 2005 memorandum opinion indicated that, depending on the facts, the scope of the HIPAA criminal provisions include covered entities and only “certain directors, officers and employees of [covered] entities, in accordance with general principles of corporate criminal liability.” Similarly, Department of Justice guidelines issued in 2005 indicated that covered entities, such as physicians, hospitals and health insurers, would face criminal penalties for unauthorized disclosures, not necessarily individuals, such as employees.

In contrast, the criminally prosecuted individuals in the most recent cases have been low-level employees whose actions would be difficult to impune to the covered entity itself. It is also significant to note that neither the Arkansas clinic or UCLA Medical Center have yet been charged in connection with the case. Similarly, while previous cases have included additional charges, including fraud and identity theft, it is noteworthy that each of these cases was brought solely for unlawful privacy disclosure under HIPAA.

While employees are increasingly targeted for improper use of patient information, covered entities also may be investigated and held civilly liable for negligence where such entities do not have in place proper privacy controls. For example, in July 2008, Seattle-based Providence Health & Services entered into a Resolution Agreement with HHS to settle potential HIPAA violations in connection with security lapses that allowed medical records of 386,000 patients to be stolen. Providence’s home services division stored these patients’ records without protective encryption on computer disks and digital tape that an employee had access to take home at night. This information was stolen from the employee’s car in two separate break-ins. Pursuant to the Resolution Agreement, Providence was required to, among other things, pay $100,000; implement a corrective action plan to safeguard patient information; train employees on safeguards; and file compliance reports for three years.

Covered entities can avoid criminal and civil sanctions against themselves and their employees for wrongful disclosure of patient information under HIPAA if they have adequate protections in place. Accordingly, covered entities should focus on developing staff training and implementing safeguards to reduce and prevent data breaches. Furthermore, covered entities should regularly educate and reinforce to employees the importance of maintaining patient confidentiality.

Correspondingly, covered entities should develop policies and procedures for effective logging practices for employees who access private patient information. Such logging procedures promote better reporting regarding access to electronic patient medical records. Effective log management for HIPAA is accomplished by having in place a logging system that features the following characteristics:

• Automatic collection and consolidation of log data;
• Automatic analysis of the data and generation of reports related to protected health information control and access;
• Regular event management, including monitoring for unauthorized software, login attempts or other suspicious behavior and discrepancies; and
• Effective identification and response to incidents.

To maintain the integrity of private patient information, a covered entity must maintain adequate security controls to monitor the access and use of such information. To that end, senior management must work together to develop clear state-