

GOVERNMENT CRACKS DOWN ON HIPAA COMPLIANCE BY COVERED ENTITIES

In July 2008, for the first time, a covered entity under the HIPAA Privacy and Security Rules was forced to make a \$100,000 payment to the government and agreed to subject itself to three years of supervision by Health and Human Services ("HHS") for losing unencrypted laptops and backup data. Government officials announced the payment and corrective action plan ("CAP") in July. Although they claim the payment was not a "fine," the payment is a major warning to covered entities that the government is getting more aggressive in regard to HIPAA privacy and security compliance.

The CAP and payment are part of a resolution agreement between HHS and Providence Health & Services to settle potential violations of HIPAA Privacy and Security Rules. The agreement was developed by the Office for Civil Rights ("OCR") and Centers for Medicare & Medicaid Services ("CMS"). Signaling its intent to step-up enforcement of HIPAA and to go after particularly egregious violations, the agreement goes beyond the action usually taken by the OCR. This is the first time the HHS has required a resolution agreement and the first time a CE is making a payment.

Although the payment is not technically a fine, the \$100,000 amount "was based upon the potential civil money penalties had this case proceeded with formal enforcement," stated Susan McAndrew, OCR's deputy director for health information privacy. The investigation was initiated after a series of incidents between September 2005 and March 2006 where electronic information that was not encrypted or otherwise properly safeguarded was lost or stolen. Over five different dates, backup tapes, optical disks and laptops, were taken from the Providence premises and left unattended. All contained unencrypted electronic protected health information. The media and laptops were then either lost or stolen compromising the private health information of over 386,000 patients.

According to McAndrew, the CAP "reinforces the point that effective compliance means more than just having written policies and procedures. To protect the privacy and security of patient information, covered entities need to continuously monitor the details of their execution, and ensure that these efforts include effective privacy and security staffing, employee training and physical and technical features."

While the \$100,000 payment may seem steep, the biggest cost of non-compliance is the great harm to a CE's reputation if the breach becomes public. It underscores the notion that CEs absolutely need to prepare for the potential that a privacy complaint could lead to serious financial costs associated with a CAP and the imposition of a "fine." The best way for a CE to prepare is to make sure it is in full compliance with the current HIPAA privacy and security regulations.

The recent up-tick in HIPAA compliance enforcement, including the hiring of private auditors by CMS, means that no physician or practice administrator can ignore the potential significant expenses of HIPAA non-compliance. While the cost of compliance may at times seem high, this expenditure could pale in comparison to the damage to your practice's reputation and the resulting loss of revenue. Now is the time to be proactive in reviewing your HIPAA compliance activities, which may have fallen by the wayside in recent years. Following is a brief review of the HIPAA Privacy and Security Rules. Contact the attorneys at Parsonage Vandenack Williams LLC to review the legal aspects of your HIPAA compliance initiatives and to stay in front of new laws and regulations affecting your practice.

A SUMMARY OF THE PRIVACY AND SECURITY RULES

A. The Privacy Rule

The Privacy Rule took effect in early 2003, and compliance with the Privacy Rule is required on and after April 14, 2003, for most covered entities. The purpose of the Privacy Rule is to establish minimum Federal standards for protecting the privacy of individually identifiable health information. Covered entities, which must comply with the Rule, are health plans, health care clearinghouses, and certain health care providers. Covered entities may not use or disclose Protected Health Information (“PHI”) except as allowed or required under the provisions set forth in the Privacy Rule. The Privacy Rule gives certain rights to patients, including the right to access and amend certain health information and the right to obtain a record of when and how their PHI has been shared with others for specific purposes. Additionally, the Privacy Rule establishes administrative requirements for covered entities. As evidenced above, covered entities that fail to comply with the Privacy Rule may face civil monetary penalties, criminal monetary penalties, and/or imprisonment.¹

Under the Privacy Rule, covered entities may disclose PHI without the patient’s authorization for purposes of treatment, payment, and health care operations, which includes many of the daily activities of providers and health plans. Still, there are certain instances where a covered entity must obtain written authorization from the patient before releasing PHI. These include PHI used for marketing purposes or situations where psychotherapy notes are involved. Moreover, the Privacy Rule requires covered entities to give public notice of their privacy practices in both electronic and hard copy form. Covered entities that directly treat patients must make a good faith effort to obtain written acknowledgment from patients that they have received the privacy practices notice.

B. The Security Rule

The final Security Rule was issued in 2003 and differs from the Privacy Rule because it only applies to Electronic Protected Health Information (“E PHI”). The Security Rule addresses the administrative, physical, and technical safeguards required for compliance. Administrative safeguards are the policies and procedures a covered entity must utilize in order to demonstrate HIPAA compliance. These include policies that determine which employee may access E PHI, how access is granted, and training for employees who handle E PHI. The physical safeguards require a covered entity to control physical access to E PHI, which means that a covered entity must restrict access to computer equipment, require physical and electronic access controls, and maintain detailed policies in regard to workstation use. Lastly, technical safeguards include controlling access to computer systems and protecting electronic communications that contain PHI. Two main requirements are that the system utilizes a form of encryption for electronic communications and a method for authenticating the other electronic party to the communication. Aside from those provider organizations and health plans that are large enough to have their own technology staff, smaller covered entities will usually need to hire outside experts to make sure that their system complies with the Security Rule requirements.

© 2009 Parsonage Vandenack Williams LLC
For more information, contact info@pvwlaw.com

¹ *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*, U.S. Department of Health and Human Services, last modified 7/13/04, < http://privacyruleandresearch.nih.gov/pr_02.asp>.