LAW OFFICES OF
GOODELL · STRATTON
EDMONDS & PALMER
ESTABLISHED 1881 LLP

By: Cody G. Robertson, Associate Attorney

HIPAA Compliance, Revisited

I. Introduction

The increasing use of new technologies in the transmission of health information holds the promise of significant advancement in the way health care is delivered in the years to come. However, any degree of enthusiasm must be tempered with an abundance of caution, as history has shown that every advance in the transmission of health information is accompanied by a host of new ways in which patient privacy may be unwittingly compromised by well-meaning providers.

It was, in part, recognition of this reality that prompted Congress to enact the Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA. A component of HIPAA, the Security Rule, requires that covered entities, including both individual and institutional providers, put into place certain safeguards to protect the integrity, availability and confidentiality of protected health information (PHI) and electronic protected health information (ePHI).

II. CMS enforcement of HIPAA

In 2003, the U.S. Department of Health and Human Services (HHS) delegated to the Centers for Medicare and Medicaid Services (CMS) (1) the authority and responsibility to interpret, implement and enforce the HIPAA Security Rule provisions; (2) the authority to conduct compliance reviews and to investigate and resolve complaints of HIPAA Security Rule noncompliance; and (3) the authority to impose civil monetary penalties for a covered entity's failure to comply with the Security Rule. This delegation of authority became effective in February 2006.

On October 27, 2008, the HHS Office of Inspector General (OIG) released a report entitled, *Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight* (the "Review"). In a nutshell, the OIG found that, by relying solely on complaints to identify noncompliant covered entities, CMS had failed to adequately implement the Security Rule. The Review recommended that, in addition to investigating complaints, CMS also establish policies and procedures for conducting Security Rule compliance audits of covered entities. CMS vocally disagreed with the OIG's findings following the release of its Review. However, at that same time CMS was busy executing a contract to begin conducting compliance audits of covered entities.

III. The lesson for providers

Because their own professional ethics have required them to safeguard patient privacy since the days of Hippocrates, physicians, more so than other covered entities such as insurers and group plans, had a relatively painless transition into compliance with the initial minimum requirements of HIPAA. Unfortunately, the result is that many physicians have become somewhat complacent in their compliance efforts. One of HIPAA's oft-neglected provisions requires covered entities to regularly review their security policies and procedures to ensure they continue to serve their intended purpose. The recent OIG Review and the subsequent indication that CMS will step up its investigative and audit activities in the coming weeks and months should serve as a warning to providers that now is the time to pay heed and review those security policies and procedures.

IV. Electronic communication

In a Security Guidance concerning the electronic communication of health information, CMS stresses that covered entities should be "extremely cautious" in their use of, or access to, ePHI by remote means such as laptops, smartphones and other portable technology. Given the increasing practice of telemedicine, e-prescribing and other electronic communications in medicine, electronic communication seems as good a place as any to begin reviewing your policies and procedures.

Your review should begin by evaluating the need for off-site use of and access to ePHI. Although often convenient, accessing ePHI remotely increases the vulnerability of that information exponentially, and thus should be done only when necessary.

Your review should also take into account the risk associated with your level of remote use of and access to ePHI. Whereas a physician who practices in multiple locations and routinely accesses e-prescribing applications from a PDA runs a relatively high risk of that information being compromised, a physician whose solo practice uses a paper-based record system and transmits little if any information electronically faces no such risk. The level of vulnerability created by your practice methods should dictate the extent and type of security measures you employ.

Any compliance program is only effective insofar as it is communicated to everyone to which it applies. Thus, the final component of your review should address the ways by which employees and business associates are made aware of and trained in your policies and procedures regarding the remote use of and access to ePHI. Training programs should be in place as well as a sanctions policy to address incidents of noncompliance.

The CMS HIPAA Security Guidance offers a number of specific risks relating to the remote use of and access to ePHI and corresponding strategies for managing those risks. It can be accessed at www.cms.hhs.gov/SecurityStandard.

V. Conclusion

While the benefits of new, more efficient methods by which to transmit health information are numerous and manifest, those benefits must be carefully weighed against the risks that are also invariably created. It is imperative that providers adopt policies and procedures to ensure that protected health information is handled appropriately. If you have any questions about your security policies and procedures, you should contact an experienced health law attorney.

This article was originally published in Vol. 1 No. 5 of Greater Kansas MD News published by Sunshine Media, Inc.