# PUBLICATION

## Pharmacies: Watch Out for Future HHS Crackdowns on Security Rule Violations

**April 6, 2015**

As we all know by now, HIPAA[1] required the Secretary of the U.S. Department of Health and Human Services (HHS) to adopt regulations protecting the privacy of "protected health information" (PHI). HHS responded to that requirement by adopting what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule.

The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards to protect the privacy of PHI. The Security Rule, or Security Standards for the Protection of Electronic Protected Health Information, protects a subset of information protected by the Privacy Rule, which is all PHI held or transferred in electronic form (e-PHI). The Security Rule does this by describing the administrative, physical and technical safeguards necessary to ensure the confidentiality, integrity and availability of e-PHI.

A 2009 law called the Health Information Technology for Economic and Clinical Health (HITECH) requires, among other things, that HHS provide for periodic audits of covered entities to check their compliance with HIPAA requirements. The HHS Office for Civil Rights (OCR) has responsibility for enforcing both the Privacy Rule and the Security Rule. In November 2013, the Office of the Inspector General (OIG) issued a report finding that the OCR was not meeting all federal requirements in its oversight and enforcement of the Security Rule. In particular, the OIG found that OCR had not complied with HITECH's requirement that it provide for periodic audits of covered entities to ensure their compliance with the requirements of the Security Rule.

Following the release of the OIG's findings, OCR audited a number of covered entities and stepped up its HIPAA enforcement activities significantly. Some of the OCR's activities since the OIG's release of its report criticizing the OCR included settlements with various covered entities for Security Rule violations. In two settlements that arose out of the theft of unencrypted laptop computers containing e-PHI, the covered entities were required to pay a total of $1,975,220 in fines for Security Rule violations. In two other settlements arising out of a failure to secure e-PHI on network computers, the covered entities were required to pay a total of $4,800,000 in fines for Security Rule violations.

In June 2014, a chief regional counsel with the OCR warned covered entities and their business associates to be ready for aggressive punishment by the OCR, and he reportedly predicted that the $10 million in HIPAA fines levied during the then-preceding 12-month period would be substantially less than the HIPAA fines he expects the OCR to impose through June 2015.

Pharmacies are subject to the same HIPAA fines as any other HIPAA-covered entity and rank fifth among HIPAA-covered entities that OCR requires to take corrective action to comply with the Privacy and Security Rules. OCR prepared a list of 1,200 companies for a new round of HIPAA audits that began at the end of 2014 and have continued into 2015. Two-thirds of the companies on the list are HIPAA-covered entities such as pharmacies and nursing homes, and the balance are business associates – those organizations that store or process PHI maintained by covered entities. Audits conducted to check compliance with the Security Rule will focus on compliance with the rule's administrative, physical and technical safeguards. Fines for willful neglect violations not corrected within 30 days can be up to $50,000 per violation. Intentional violations or violations that involve fraud are subject to more severe penalties, including prison.

We can expect HHS to continue to surprise HIPAA-covered entities, including pharmacies, with big-ticket penalties throughout 2015. Many of the violations of HIPAA's Security Rule for which covered entities have been sanctioned to date could easily have been avoided by (1) securing laptop computers and other portable devices, and (2) performing a comprehensive risk analysis of security management processes on an ongoing basis, identifying the risks and implementing appropriate security measures.

To better protect your pharmacy operations from potential violations of HIPAA's Security Rule, we recommend the following:

- Appoint a trusted employee as your Security Official, responsible for developing and implementing your security policies and procedures. That appointment should be documented.
- Have your Security Official review the six educational programs sponsored by the OCR on compliance with Privacy and Security Rules. Of particular relevance to complying with the Security Rule are the programs "Your Mobile Device and Health Information Privacy and Security," and "Understanding the Basics of HIPAA Security Risk Analysis and Risk Management." These programs are available here.
- Invest in available software to assist your Security Official with Security Rule compliance.
- Have your Security Official study the "Audit Program Protocol" and conduct a self-audit of your pharmacy's compliance with the Security Rule.

---

[1] Health Insurance Portability and Accountability Act of 1996 (P.L. No. 104-191, 110 Stat. 1936 (1996)).