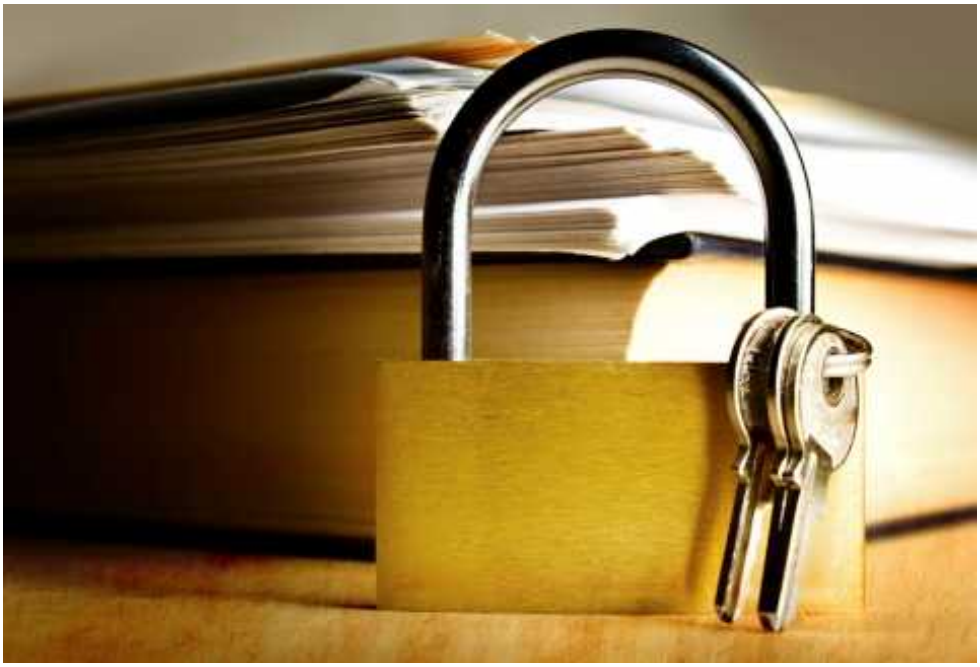
HIPAA Security Policies - "What do you mean, 'We forgot to adopt them'?"

Forrest W. Campbell, Jr.
November 1, 2012



HIPAA has returned as a key compliance area. And some providers may be at significant risk because they never adopted HIPAA "security" policies to implement the HIPAA "security" rules.

What am I talking about? Let's start with a short review of the HIPAA rules. The HIPAA "privacy" rules are what most people think of when you mention HIPAA—they govern the general confidentiality of PHI by regulating how providers use and disclose PHI and by establishing patients' rights concerning PHI. They require "notices of privacy practices", "business associate agreements", and "minimum necessary" uses and disclosures (among other things).

The "privacy" rules were effective on April 14, 2001, and most providers had two years to comply. Compliance included adopting numerous HIPAA "privacy" policies. In response, throughout the nation, providers worked diligently and adopted HIPAA "privacy" policies. All of that was good....

But several years later, along came the HIPAA "security" rules, and a fair number of providers seem to have fallen asleep and not adopted and implemented policies for those rules. Effective April 21, 2003, CMS adopted the HIPAA "security" rules—which address the administrative, physical, and technical safeguards required for protecting the security of electronic PHI. These rules are completely separate and distinct from the "privacy" rules, and providers had to comply with these rules by April 21, 2005.

The "security" rules impose extensive requirements to protect the security of the electronic PHI a provider stores, uses, and transmits. These rules impose over 60 very specific security requirements—including requirements that providers conduct a documented "risk analysis", appoint a security officer, document physical repairs and modifications to the

facility (such as doors and locks), have disaster recovery plans, have automatic computer logoffs after a period of inactivity, have procedures for periodically changing user passwords, and have procedures to monitor login attempts.

Moreover, providers must have written policies that implement the numerous security requirements, must document their "risk analysis" (and update it periodically), and must retain a copy of the policies and analysis for at least six years.