

# HIPAA Security Rule – The “Other Shoe” of HIPAA

## Introduction

When the HIPAA Privacy Rule was issued, to much fanfare, by the U.S. Department of Health and Human Services in 2002, most health care providers diligently implemented the required privacy policies and procedures prior to the April 14, 2003, compliance deadline. However, some providers have not implemented security policies and procedures as required by the HIPAA Security Rule, which was issued in 2003. The compliance deadline for the Security Rule was April 20, 2005.

## What the Security Rule Covers

The Security Rule covers electronic Protected Health Information (PHI), as defined by HIPAA. Items it does not cover include oral and written communications, paper-to-paper faxes, and voice mail messages. Remember, however, that the HIPAA Privacy Rule does apply to PHI in all forms and formats.

## What the Security Rule Requires

Generally speaking, the Security Rule requires steps to ensure the confidentiality and integrity of all electronic PHI. It mandates protection against any reasonably anticipated threats or hazards to the security or integrity of such information. The threats or hazards the Security Rule is intended to protect against range from computer hacking to natural disasters to nosy medical office visitors glancing at computer workstation screens.

The Security Rule's specific requirements break down into five broad categories: 1) administrative safeguards, 2) physical safeguards, 3) technical safeguards, 4) organizational requirements, and 5) policies and procedures and documentation requirements.

The safeguards categories contain standards and detailed "implementation specifications" for the standards that are either "required" or "addressable." Required means required. For example, a sanctions policy for employees who fail to password protect their BlackBerrys or Treos if they use them for PHI would be required, period. Addressable means the entity must consider whether and to what extent the specification would be "reasonable" and "appropriate" in the entity's particular environment when analyzed in reference to its likely contribution to protection of electronic PHI. For example, encryption of electronic PHI on an employee's BlackBerry or Treo would be an "addressable" specification.

However, addressable does not mean purely optional. The Security Rule requires that if an entity declines implementation of an addressable implementation specification, it must document why it has so declined, and either a) implement an equivalent alternative measure or b) otherwise meet the standard, and, finally, document why the alternative is equivalent or why the standard is otherwise met. In the case of encryption, for example, it is difficult to imagine what alternative measure (short of prohibiting the electronic conveyance of PHI) would serve as an equivalent or how the relevant access control standard could otherwise be met. Therefore, it is advisable to use encryption.

Many of the addressable specifications, such as automatic logoff for employee workstations, are no brainers because it is easier simply to implement them than to come up with equivalent alternative measures or show the standard is otherwise met. Nevertheless, the covered entity will still have considerable leeway in implementing the specifications. Sticking with the example of automatic logoff, the covered entity will have to decide how much time workstations remain inactive before automatic logoff occurs.

Even the required specifications afford substantial discretion to the covered entity. For example, all covered entities are required to have data backup plans, disaster recovery plans, and emergency mode operation plans. Instead of listing the contents of such plans, the Security Rule merely directs the covered entity to generate the plans appropriate to its size and complexity, as well as the cost of security measures relative to size and the probability and criticality of the risk to the data.

Finally, the covered entity is required to maintain formal written policies and procedures and to document compliance with those actions, activities, or assessments required to be documented by the Security Rule. Penalties for non-compliance with the Security Rule include significant civil and criminal monetary penalties and jail time.