TMA Privacy Office Information Paper

The Who, What, When, and Where of the Security Rule

HIPAA Security◆November 2003

Who must comply with the Security Rule and when?

All covered entities must comply with the Security Rule. HIPAA defines a covered entity as all (a) health plans, (b) health care clearinghouses, and (c) health care providers who "engage electronically in the transactions for which standards have been adopted." The HIPAA definition of a Health Plan specifically cites the military's health plan as a covered entity. The military treatment facilities (MTFs) and other military providers treating the military and beneficiary population utilize a number of the standard transactions, making them covered entities as well. DoD covered entities must comply with the Security Rule by April 21, 2005.

What is covered by the Security Rule?

HIPAA defines protected health information (PHI) as individually identifiable health information that is maintained or transmitted in any form or medium, except for information in records covered by the Family Educational Rights and Privacy Act and employment records held by a covered entity in its role as employer. The HIPAA Privacy Rule covers PHI in all forms (paper, oral and electronic). The HIPAA Security Rule applies only to PHI that is maintained or transmitted in electronic form (EPHI).

The Security Rule requires protection of all EPHI, regardless of where or how it is used. The rule does not differentiate between internal and external transmissions, "data at rest" (stored or in process) or "data in motion" (in transmission). Security must apply to all electronic "systems" which HIPAA defines as "interconnected set[s] of information resources under the same direct management control that share common functionality. A system normally includes hardware, software, information, data, applications, communications and people." (164.304) This broad applicability gives the Security Rule a unique organizational slant and accounts for the comprehensiveness of the Rule's administrative, physical and technical safeguard requirements.

Almost all electronic devices today contain microprocessors. Although the Security Rule applies to any electronic computing device, DHHS has clarified that it intends to include only "software programmable computers, for example personal computers, minicomputers, and mainframes." (Final Rule, p.8342) Laptops, tablet computers, PDAs and other portable computing devices are included, whether they are a stand alone device or are linked to another system or network by wire or wireless connection. Copy machines, fax machines and telephones are not included as long as they are not networked or part of a computer system. For example, a stand alone copy machine is not included but a copy machine that is also a network printer is. While telephone communications and fax transmissions are not covered, telephone voice response and "faxback" systems (where a request for information from a computer is made via voice or telephone keypad input, with the requested information returned via fax) are covered by the Security Rule. It is important to note however, that while things like voice mail and paper to paper faxes are not covered by the Security Rule, the Privacy Rule requires protection of all PHI in any form.

Where must I apply the Security Rule?

A covered entity is expected to apply security safeguards to its entire "facility" — defined as the "physical premises and interior and exterior of [its] building[s]" — and the "systems" therein.

TMA Privacy Office Information Paper

The Who, What, When, and Where of the Security Rule

However, it does not end there. The DHHS explains that "a covered entity's responsibility to implement security standards extends to the members of its workforce, whether they work at home or on-site." (Final Rule, p. 8339) A covered entity must have policies and procedures that apply HIPAA standards to employees who take work that contains EPHI home, or who connect to the covered entities systems from home or elsewhere, such as transcriptionists, claims processors, physicians and researchers.