NGA Center for BEST PRACTICES

Fact Sheet

THE SECURITY RULE

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established a federal floor of patient protections and industry standards to govern the health care marketplace. At the same time, HIPAA attempted to preserve the ability of states to create and enforce their own laws that exceed those federal boundaries.

WHAT IS THE HIPAA SECURITY RULE?

HIPAA directed the U.S. Department of Health and Human Services (HHS) to promulgate a regulation—the Security Rule—to ensure the integrity, safety, and security of patient medical information when collected, exchanged, or otherwise used in the health care marketplace. More specifically, the Security Rule:

- Establishes the organizational standards—administrative, physical, and technical—that covered entities must adopt to prevent unauthorized access to patient health information; and
- Assures the safety and integrity of patient health information when consumers exercise their health privacy rights (under the HIPAA Privacy Rule).

WHO IS COVERED?

Entities that perform any of the following covered functions:

- Individual or group **health plans** (or programs) that provide for or pay the cost of health benefits directly, through insurance, or otherwise;
- **Health care providers** (or suppliers) who furnish, bill, or receive payment for medical or other health services or supplies (and who also conduct certain health care transactions electronically); and/or
- **Health information clearinghouses** that process or facilitate the processing of electronic health information into standard or nonstandard formats.

Through mandatory contracts (or trading partner agreements), covered entities are expected to reasonably ensure that their **business associates**—those with whom they exchange information or contract for administrative and other services—are also HIPAA compliant. Covered entities are not required to monitor compliance by their business associates, but will be held liable for failing to require corrective action or terminate the relationship if a violation is discovered.

WHAT IS COVERED?

Electronic protected health information (E-PHI), which by definition:

- is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse;
- relates to the past, present, or future physical or mental health or condition of the individual; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual;
- identifies the individual directly or provides a reasonable basis to believe that the information can be used to identify the individual; and
- is transmitted and/or maintained in an electronic medium.

Unlike the Privacy Rule, the Security Rule applies only to PHI that is transmitted or maintained electronically. It does not apply to PHI transmitted or maintained in any other medium (written or verbal).

COMPLIANCE DEADLINE

The deadline to comply with the Security Rule is **April 21, 2005** (2006 for small plans).

ENFORCEMENT AND PENALTIES

Noncompliance can trigger civil monetary penalties (CMPs) of up to $100 for each HIPAA violation (up to $25,000 per person). The federal Centers for Medicare and Medicaid Services (CMS) will enforce the Security Rule.

CRITICAL ISSUES

States have primary responsibility for:

- evaluating how PHI is electronically collected, stored, used, and/or shared throughout state government;
- determining which agencies and programs meet the *federal* definition(s) of a covered entity;
- establishing administrative, physical, and technical safeguards in areas vulnerable to unauthorized access; and
- obtaining reasonable assurances that business associates are also in compliance.

State-administered covered entities must meet 18 standards—administrative, physical, and technical—to successfully comply with the Security Rule. The standards can be met using a combination of:

- 14 *mandatory* specifications (to which covered entities must adhere); and
- 22 *addressable* specifications (to be considered and implemented when appropriate).

If the addressable specifications are not appropriate, states must document why and explain what alternative measures were taken to fully implement each standard.

For additional information, visit: http://www.nga.org/center/hipaa/.

Robert J. Burns, Policy Analyst, Health Policy Studies Division, (202) 624-7729, rburns@nga.org