NGA Center for BEST PRACTICES

Fact Sheet

PRIVACY STANDARDS FOR INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

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 PRIVACY RULE?

HIPAA directed the U.S. Department of Health and Human Services (HHS) to promulgate a regulation—the Privacy Rule—to protect and enhance the right of consumers to control how their personal health information is used and disclosed. Specifically, the Privacy Rule:

- stipulates the individual rights of consumers to control their personal health information, including guaranteed access to their medical records and a clear avenue of recourse if their medical privacy is compromised;
- outlines the procedures organizations must adopt to enable patients to exercise their privacy rights, including proper notification of how their personal health information is used and shared;
- establishes the conditions under which individuals or organizations may use and/or disclose personal health information;
- sets an industry standard for disclosing only the minimum amount of information necessary to satisfy an authorized request for patient information; and
- requires organizations to appoint a privacy officer to conduct privacy assessments, create policies to protect patient privacy, train staff, and establish an internal grievance process.

WHO IS COVERED?

Covered entities include:

- **health plans,** which are individual or group plans (or programs) that provide health benefits directly, through insurance, or otherwise.
- **health care providers,** which are providers (or suppliers) of medical or other health services or any other person furnishing health care services or supplies, and who also conduct certain health-related administrative or financial transactions electronically; and
- **health information clearinghouses,** which are any public or private entities that process or facilitate processing of nonstandard health information into standard data elements.

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?

Protected health information is information from an individual that 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; and
- identifies the individual directly or provides a reasonable basis to believe that the information can be used to identify the individual.

The Privacy Rule defers to any state law that requires reporting or disclosures for specified purposes.

COMPLIANCE DEADLINE

The compliance deadline for the privacy rule is April 14, 2003 (2004 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). Individuals convicted of criminal violations can be fined up to $250,000 and receive up to ten years in prison. HHS' Office for Civil Rights (OCR) is responsible for enforcing civil violations of the Privacy Rule. Criminal violations will be investigated and prosecuted separately by the U.S. Department of Justice.

CRITICAL ISSUES

States have primary responsibility for determining which agencies and programs meet the *federal* definition(s) of a covered entity.

States must evaluate how individually identifiable health information is collected, stored, used, and shared throughout state government and establish new protocols and procedures to ensure that information remains confidential and secure.

States must determine which personal health information meets the federal definition of *protected health information*. States must also interpret the *minimum amount necessary* threshold for releasing information based on industry standards.

States must judge the relative strength of other state and federal privacy laws to determine whether those laws supercede HIPAA's privacy provisions. Where existing state and federal laws do not meet the HIPAA privacy standard, states must either enact stronger privacy laws or adopt those prescribed by HIPAA.

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