Department of Health Care Policy & Financing

HIPAA – GENERAL INFORMATION

"Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart there from, which ought not be noised abroad, I will keep silence thereon, counting such things to be as sacred secrets."

– Oath of Hippocrates, 4th Century, B.C.

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is perhaps the single most significant piece of federal legislation affecting the health care industry since the inception of the Medicare and Medicaid programs. The legislation consists of several broad and far-reaching provisions, including:

- The improvement of the portability and continuity of health insurance coverage for millions of American workers and their families.
- The prohibition on group health plans from placing certain limits or restrictions on health care coverage.
- The promotion of *Administrative Simplification* in the health care industry through the development of standards for the electronic exchange of information in order to simplify the burdens and reduce the costs of administering health care.
- The requirement that the U.S. Department of Health and Human Services promulgate rules to maintain the privacy of individuals' *Protected Health Information* and to establish security requirements to protect that information, thus enhancing the ability of consumers to control how their health information is used and disclosed.

This information sheet is intended to address the *Administrative Simplification* section of the law, more specifically the Privacy and Security Rules.

What is Administrative Simplification?

The goals of *Administrative Simplification* include protecting the privacy rights of individuals; developing standards for the exchange of electronic health care information and the security of data processing systems; and creating standard identifiers for employers, health care providers, and health plans. Specific provisions include:

- The *Privacy Rule* to protect individually identifiable health information that is transmitted or maintained in any form or medium. The compliance deadline for implementing the *Privacy Rule* was April 14, 2003.
- The *Security Rule* to ensure implementation of various safeguards to protect certain electronic health information from improper access, disclosure, or destruction. The compliance deadline for implementing the *Security Rule* is April 21, 2005.
- The *Transaction and Code Set Rule* to mandate the development and use of standardized transactions to be used in the electronic exchange of data. In addition, the Regulations require the use of standardized national code sets to identify medical conditions, treatments, procedures, durable medical equipment, and drugs. The compliance deadline for most entities for implementing the *Transaction and Code Set Rule* was October 16, 2003.

Who Is Covered?

HIPAA classifies the following as *Covered Entities* and requires their compliance:

- *Health Plans*, including individual or group plans that provide or pay the cost of medical care and includes both the Medicare and Medicaid programs.
- *Health Care Providers* who transmit any health information (including billing for health care) in electronic form in connection with the transactions covered in the Transaction and Code Set Regulations. Physicians, hospitals, physical therapists, pharmacists, and providers of home medical equipment would be included in this category.
- *Health Care Clearinghouses* that process or facilitate the processing of health information received from other entities.

The *Business Associate* of a *Covered Entity* must meet various HIPAA requirements as well. A *Business Associate* is an entity or person who performs a function or activity on behalf of a *Covered Entity*; is not an employee of the *Covered Entity*; and has access to, uses, or discloses *Protected Health Information*. A *Covered Entity* may be a *Business Associate* of another *Covered Entity*.

Department of Health Care Policy & Financing

What is Covered?

Protected Health Information is that information specifically covered by the *Privacy Rule*. It is information that meets all of the following requirements:

- It is created or received by a health care provider, health plan, health care clearinghouse, or employer; and
- It relates to the past, present, or future physical or mental health or condition of an individual; the provision [treatment] of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
- It identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual (Including: name, address, city, county, birth date, social security number, telephone number, email address, medical record number, health plan beneficiary number, and other identifiers); and
- It is transmitted or maintained in any form or medium.

Protected Health Information excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, and employment records held by a covered entity in its role as an employer.

The requirements mandated by the *Security Rule* apply only to *Electronic Protected Health Information*, which is *Protected Health Information* that is transmitted or maintained electronically

What Is the HIPAA Privacy Rule?

The *Privacy Rule* is intended to protect and enhance the right of consumers, clients, and patients to control how their health information is used and shared.

- It outlines the procedures entities must adopt to enable patients/clients to exercise their privacy rights, including guaranteed access to their medical records and a clear avenue of recourse if their medical privacy is compromised;
- It establishes the conditions under which individuals or organizations may use and/or disclose *Protected Health Information*;
- It sets an industry standard for disclosing only the minimum amount of information necessary to satisfy an authorized request for patient information; and
- It requires each *Covered Entity* to appoint a *Privacy Officer* to create policies to protect individual patient/client privacy, train staff, establish an internal grievance process, and serve as an information resource.

What Is the HIPAA Security Rule?

The *Security Rule* is intended to ensure the confidentiality, integrity, and availability of electronic health information collected or maintained on consumers, clients, and patients.

- It is comprehensive, technology neutral, and scalable;
- It establishes standards for the security of *Electronic Protected Health Information* used, maintained, or transmitted by *Covered Entities*; and
- It requires various administrative, physical, and technical safeguards to ensure that data is protected, to the extent feasible, from inappropriate access, modification, dissemination, and destruction.

For More Information:

United States Department of Health and Human Services, Office of Civil Rights, HIPAA
www.hhs.gov/ocr/hipaa

Privacy Officer, State of Colorado, Department of Health Care Policy and Financing
Phone: 303-866-4366