LARSON • KING, LLP
Overview of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

By: Mark A. Solheim, Esq.
Stephen P. Laitinen, Esq.
LARSON • KING, LLP
2800 Minnesota World Trade Center
30 East Seventh Street
St. Paul, MN 55101-4922
(651) 312-6500

Why Do You Need to Know About HIPAA?

As you will learn in this report, HIPAA is an amazingly comprehensive, sweeping body of federal legislation that will completely change the landscape of how health care professionals, health care insurers, casualty carriers, law firms, and corporate legal departments involved in health care issues deal with customer information privacy and security issues in the future. This report will hopefully serve as an initial guidepost of what HIPAA is, what HIPAA is intended to cover, and most importantly, what you need to do in order to come into compliance with HIPAA in the year 2003.

What is HIPAA?

Congress recognized the need for national patient record privacy standards in 1996 when it enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The law included provisions designed to save money for health care businesses by encouraging electronic transactions, but it also required new safeguards to protect the security and confidentiality of that information. HIPAA was signed into law on August 21, 1996.

The Administrative Simplification Portion of HIPAA is designed to do the following:

- Protect patients' rights;
- Improve the quality of health care; and
- Improve the delivery of health care.

HHS has also issued the regulation, *Standards for Privacy of Individually Identifiable Health Information* (the Privacy Rule), applicable to health care entities covered by HIPAA.

The Privacy Rule gives patients greater access to their own medical records and more control over how their protected health information ("PHI") is used. The rule also addresses the obligations of health care providers and health plans to protect health information.

The Office for Civil Rights (OCR) is the governmental component responsible for implementing and enforcing the Final Privacy Rule, made effective on April 21, 2001.

The Rule's compliance date is either:

- April 14, 2003 for "regular" health plans: and
- April 14, 2004 for "small" health plans.

Covered entities under HIPAA are not required to comply with HIPAA's Privacy Rule until the compliance dates set forth above.

Furthermore, HIPAA is a "going-forward" type of legislation; covered entities will **not** be required to do anything to protect PHI created **prior** to April 14, 2003 or 2004.

What Type of Health Care Transactions Are Covered Under HIPAA?

The privacy standards apply to covered entities that transmit any health information in any form in connection with the following transactions:

- Health claims information;
- Health claims attachments;
- Health plan enrollment or disenrollment;
- Health plan eligibility;
- Health care payment and remittance advice;
- Health plan premium payments;
- First report of injury;
- Health claim status;
- Referral certification and authorization; and
- Coordination of benefits.

Eight Quick Definitions Under HIPAA.

Covered entity means:

- A health plan;
- A health care provider; and
- A health care clearinghouse.

Health plan means an individual or group plan that provides, or pays the cost of, medical care.

Health care provider means:

- A provider of medical or health services; and
- Any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health care clearinghouse means:

- A third-party entity, including a billing service, re-pricing company, community health management information system, and other "value-added" networks.

Health information means:

- Any information, whether oral or recorded in any form or medium;

- 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; and

- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer means:

- An insurance company, insurance service, or insurance organization (including an HMO), licensed to engage in the business of insurance in a State and subject to State law that regulates insurance.

Business associate means:

- A person or entity who receives PHI from a covered entity to enable the business associate to perform a specific service for the covered entity.

- A *covered entity* may be a *business associate* of another *covered entity.*

Business associates include:

- Attorneys;

- Consultants;

- Accountants and actuaries;

- Third-party administrators; and

- Other vendors.

Small health plan means:

- A health plan with 50 or less employees and/or annual receipts of $5 million or less.

Administrative Simplification.

The Administrative Simplification Act has three fundamental goals:

- To protect the *privacy* of patient information;

- To provide for the *security* of patient information; and

- To allow for the *standardization* of (a) certain electronic transactions; (b) unique identifiers for each covered entity; and (c) certain code sets for PHI.

Essentially, HIPAA requires covered entities to administer health benefits in a standardized and governmentally regulated environment, and to preserve the privacy and security of personal health data.

HIPAA's Privacy Rule.

The Privacy Rule deals with "individually identifiable health information" in the following manner:

- All covered entities (health plans, health care providers, and health care clearinghouses) must comply;
- Defines the permitted and mandatory uses and disclosures of PHI;
- Provides administrative compliance rules; and
- Offers individuals rights to access and protections of their PHI.

The Privacy Rule centers upon:

- Individually identifiable health information;
- Kept or disclosed by a covered entity electronically, on paper, or orally.

However, health care data that is "de-identified" is not PHI.

Protected Health Information.

PHI is individually identifiable health information that:

- Operates as a subset of health information, i.e., demographic data;
- Is either created or received by a covered entity, and which:
- Relates either to the past, present or future condition of a person; the delivery of health care to that person; or the past, present, or future payment for the delivery of health care to that person.
- Identifies the person; or
- Provides a reasonable basis for allowing the identification of the person from the information.

The Privacy Rule's "Minimum Necessary" Requirement.

Under the Rule, covered entities must make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary to achieve the intended purpose of the use, disclosure or request.

The minimum necessary requirement does **not** apply to:

- "Routine disclosures," including insurance claims;
- "Treatment-related" exchanges of data between health care providers;
- Disclosures to the individual patient;
- Disclosures to the Secretary of Health and Human Services;
- Uses and disclosures required by law.

Patient Rights.

Under HIPAA, every person is entitled to:

- Receive an explanation of his or her privacy safeguards;
- Access to their PHI and the opportunity to request amendments to their PHI;
- The ability to grant consent before PHI is disclosed or released;
- Request an accounting of prior disclosures made by a covered entity; and
- File a formal complaint with HHS against a covered entity regarding alleged HIPAA violations or procedural irregularities.

Consent Requirements under HIPAA.

Generally, release of a person's PHI requires signed consent by that individual. However, health care providers may condition treatment to a person on receiving consent, under certain circumstances.

However, if data use and disclosure is limited to health care "treatment, payment and operations" consent is **not** required.

Authorization Requirements under HIPAA.

A covered entity's use of PHI for reasons other that for "treatment, payment, or health care operations" requires a person's specific authorization. Some key points:

- "Authorization" is not "consent."
- Disclosure is restricted to the "minimum necessary."

- Authorization form must be in "plain language."

- PHI use and disclosure must be defined, and third parties receiving PHI must be identified.

- Authorization must be dated and must have a finite expiration date.

- Patient's signature required.

HIPAA's Security Requirement.

Covered entities must establish appropriate administrative, technical and physical protections to ensure the privacy of PHI. Specifically, the covered entity must have procedures in place to guarantee that:

- Health care data is not used or disclosed in violation of the Privacy Rule;

- A covered entity's members or a covered entity's business associates not authorized to access or use PHI will have the ability to do so.

- Covered entities must appoint a "privacy officer" to oversee procedures and enforcement of the Privacy Rule on site.

HIPAA and State Privacy Laws.

HIPAA generally preempts contrary State laws.

However, State laws are not preempted if:

- State law is more stringent than HIPAA;

- HHS denies a request for an exemption, on a permitted basis;

- The state law relates to a public health issue, public licensing, or a health plan audit; and

- ERISA interplay still to be decided under HIPAA.

Federal Civil Penalties.

Covered entities that violate HIPAA may be subject to the following civil penalties:

- Up to $100 per violation, for a maximum of $25,000 per year for multiple violations of the same standard under HIPAA;

- Penalty caps only apply to a violation of one provision at a time;

- HHS enforcement through the Office of Civil Rights (OCR), with power to engage in "compliance audits."

Federal Criminal Penalties.

Covered entities that knowingly and wrongfully disclose or receive individually identifiable health information in violation of HIPAA may face the following penalties:

- Up to $50,000 fine;
- 1 year in prison;
- Or both.

If an offense is committed under false pretenses:

- Up to $100,00 fine;
- Up to 5 years in prison; and
- Or both.

If a covered entity is guilty of the offense of an intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm:

- Up to $250,000;
- Up to 10 years in prison; and
- Or both.

The Department of Justice enforces these civil and criminal penalty rules.

Summary of Action Areas.

Well, now that you possess a working knowledge of HIPAA, what do you need to do if you are a "covered entity" or a "business associate" of a covered entity? First, all covered entities will have to undertake the following tasks:

Administrative Requirements:

- Appoint privacy officer;
- Draft privacy policies and procedures;
- Implement training programs;
- Maintain compliance areas;
- Perform ongoing monitoring.

Individual Patient Rights Procedures:

- Establish process for logging "non-routine" uses and disclosures;
- Appoint contact person for inquiries/complaints;
- Draft authorization and consent forms;
- Distribute "notice of rights" to individual customers;
- Establish process for handling and responding to requests for access.

Uses and Disclosures Procedures:

- Identify covered entities;
- Identify all uses and disclosures of PHI to determine whether current procedures comply with the Rule;
- Establish barriers between covered and non-covered entities and between different lines of communication, i.e., PHI needed to monitor casualty claims;
- Document internal and external uses of PHI.

Minimum Necessary Requirement Procedures:

- Identify current uses of PHI and evaluate minimum necessary requirements to be in compliance with the Rule.

Business Associates Procedures:

- Identify and catalogue all business associates;
- Contract language is required between covered entity and business associate to ensure that HIPAA Privacy Rule is "acknowledged" by business associate, and that business associate agrees to not use or disclose PHI in violation of HIPAA;
- However, a covered entity is not required to perform "due diligence" as to business associate's compliance with Rule, nor will a covered entity be held responsible (at least as HIPAA is currently drafted) for a business associate's non-compliance with the Privacy Rule.

Although HHS and the Bush Administration have not yet opined on the issue, health care insurers, casualty carriers, law firms and corporate legal departments will more than likely be categorized, on a case-by-case basis, as "business associates" of covered entities.

WHAT YOU NEED TO DO RIGHT NOW.

LARSON • KING, LLP will continue to monitor ongoing HIPAA compliance developments. There will likely be further clarification areas on the Privacy Rule prior to April 14, 2003, the date for final compliance for most covered entities. There may also be additional sets of HIPAA regulations. In addition, your particular vendors are probably engaged in compliance efforts at present; you may wish to contact them immediately to find out exactly what steps each is taking to come into compliance under HIPAA.

Mark A. Solheim, Esq.
Larson • King, LLP
2800 Minnesota World Trade Center
30 East Seventh Street
St. Paul, MN 55101-4922
(651) 312-6503
msolheim@larsonking.com

Stephen P. Laitinen, Esq.
Larson • King, LLP
2800 Minnesota World Trade Center
30 East Seventh Street
St. Paul, MN 55101-4922
(651) 312-6517
slaitinen@larsonking.com