Legal – HIPAA

Health Insurance Portability and Accountability Act [HIPAA]

What is HIPPA?
The goals and objectives of this legislation are to streamline industry inefficiencies, reduce paperwork, make it easier to detect and prosecute fraud and abuse and enable workers of all professions to change jobs, even if they (or family members) had pre-existing medical conditions.

1. Assure health insurance portability by eliminating job-lock due to pre-existing medical conditions.
2. Reduce healthcare fraud and abuse.
3. Enforce standards for health information.
4. Guarantee security and privacy of health information.

Who is affected by HIPAA?
HIPAA directly regulates three types of 'covered entities.' These include health care providers, health care clearinghouses, and health plans. Included within the category of health plans are employer group health plans. Therefore, although employers are not directly regulated by HIPAA, the health plans they sponsor are. If you provide health benefits to your employees, you will be affected by HIPAA to some degree. The extent to which you will be impacted depends on such factors as whether your self-insure your health care benefits or provide your health benefits solely through an insurance contact.

Regulations of HIPAA.

HIPAA regulations are structures as five major provisions or titles:

Title 1: Health Insurance Access, Portability, and Renewability

Title 2: Preventing Healthcare Fraud and Abuse, Administrative Simplification, Medical Liability Reform

Title 3: Tax Related Health Provisions

Title 4: Application and Enforcement of Group Health Insurance Requirements

Title 5: Revenue Offsets
The purpose behind the five titles falls into two major categories: Administrative Simplification and Insurance Reform. The Administrative Simplification sections are most relevant to health care providers while the Insurance Reform sections are relevant to payers.

Insurance Reform.
The Insurance Reform section of HIPAA has been in effect since 1997 and has changed the

practices of health plans and insurers regarding Portability and Continuity of health coverage in the following ways:

- Provides limitation on pre-existing condition exclusions.
- Prohibits discrimination against individuals based on health status.
- Helps individuals to keep health insurance when they change jobs.
- Prevents insurers from imposing pre-existing condition exclusions on new members when they have prior creditable coverage.
- Guarantees once employers or individuals purchase health insurance, those policies will be renewed.

Administrative Simplification.

The Administrative Simplification section of HIPAA consists of standards for the following areas: electronic transactions, privacy, and security. The purpose is to:

- Reduce the costs of administrative overhead estimated at $.26 of every health care dollar.
- Improve the efficiency and effectiveness of the national health care system.
- Reduce fraud abuse.
- Protect privacy of health information.
- Protect patient's rights.
- Provide appropriate level of protection for privacy and security of patient health information.
- Improve quality of patient care via improved clinical data access.
- Enhance information availability for decision making.
- Reduce vulnerability of Internet-based technology to security breaches.

Does HIPAA apply to a small employer?
HIPAA's group market rules apply to every employer group health plan that has at least two participants' who are current employees. Further, States have the option of applying the group market rules to groups of one.

How will HIPPA benefit me as a small employer?
HIPPA guarantees access to health coverage for small employers. Small firms (50 or fewer employees) are guaranteed access to health insurance, and generally, no insurer can exclude a worker or family member from employer-sponsored coverage based on health status. Insurers are required to renew coverage to all groups, regardless of the health status of any member.

As a small employer, how am I going to make this work?
If you purchase group health insurance coverage, your insurer should be able to handle HIPAA information collection activities and certificate issuance for you. Talk to your insurer to find out how you can work out the process-related issues together.

HIPAA changes how plans and issuers may apply pre-existing condition exclusions. What does this mean?

A "pre-existing condition exclusion" is a limitation or exclusion of health benefits based on the fact that a physical or mental condition was present before the first day of coverage. However, HIPAA limits the extent to which a plan or issuer can apply a pre-existing condition exclusion.

Pre-existing condition exclusion is limited to a physical or mental condition for which medical advice, diagnosis, care, or treatment was recommended or received within the six-month period ending on the enrollment date in a plan or policy.

During the pre-existing condition exclusion period, the plan or issuer may opt not to cover or pay for treatment of a medical condition based on the fact that the condition was present prior to an individual's enrollment date under the new plan or policy. (The plan or issuer must, however, pay for any unrelated covered service or condition that may arise once coverage has begun.) The enrollment date is the first day of coverage, or if there is a waiting period before coverage takes effect, the first day of the waiting period.

A group health plan can apply a pre-existing condition exclusion for no more than twelve months after an individual's enrollment date. Any pre-existing condition exclusion must be reduced by an individual's prior creditable coverage. No pre-existing condition may be applied to an individual who maintains continuous creditable coverage (without a break of sixty-three or more days) for twelve months.

Does previous health coverage count for coverage under HIPAA?
Yes. In HIPAA terminology, this is called creditable coverage. This is one of the law's main benefits. The concept of creditable coverage is that an individual should be given credit for previous health coverage against the application of a pre-existing

How do employers comply with HIPPA?
There are three major aspects to the HIPAA Administrative Simplification requirements: Standardized Healthcare Transactions and Code Sets; the Health Information Privacy Rule; and the Health Information Security Rule. Each of these three major rules has a separate compliance date.

The first rule for Transaction and Code Sets mandates that the health care industry be conducted according to standard rules. The second, and probably most significant HIPAA compliance rule is the Privacy Rule.

The **Privacy Rule** is intended to protect the privacy of individually identifiable health information in the hands of covered entities, regardless of whether the information is, or has been, in electronic form. The rule establishes the first "set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation." The Privacy standards:

- Gives patients new rights to access their medical records, restrict access by others, request changes, and to learn how they have accessed.
- Restrict most disclosures of protected health information to the minimum needed for healthcare treatment and business operations.
- Provide that all patients are formally notified of covered entities' privacy practices.
- Enable patients to decide if they will authorize disclosure of their protected health information (PHI) for uses other than treatment or healthcare business operations.
- Establish new criminal and civil sanctions inform improper use or disclosure of protected health information (PHI).

- Establish new requirements for access to records by researchers and others.
- Establish business associate agreements with business partners that safeguard their use and disclosure of protected health information (PHI).
- Implement a comprehensive compliance program, including:
    - Assigning a "Privacy Officer" that will administer the organizational privacy program and enforce compliance.
    - Training all members of the workforce on HIPAA and organizational privacy policies.
    - Updating systems to ensure they provide adequate protection of patient data.
    - Developing and implementing privacy policies and procedures.

The third rule, the **Security Rule** provides for a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual. The Security Rule requires covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) the covered entity creates, receives, maintains, or transmits. It also requires entities to protect against:

- any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information (ePHI);
- to protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule;
- and ensure compliance by the workforce.

Required safeguards include application of appropriate policies and procedures, safeguarding physical access to electronic protected health information (ePHI), and ensuring that technical security measures are in place to protect networks, computers, and other electronic devices.

Compliance Dates.

Most entities have twenty-four months from the effective date of the final rules to achieve compliance. Normally, the effective date is sixty days after a rule is published. The compliance date for:

- Tranactions Rule compliance date is October 16, 2003
- Privacy Rule compliance date is April 14, 2003
- Security rule compliance date is April 15, 2005
- Employer Identification Standard compliance date is July 30, 2004. [This rule/standard adopts an employer's tax ID number or employer identification number (EIN) as the standard for electronic transactions.]

What penalties might employers face for non-compliance of HIPAA?

Unfortunately, HIPAA's enforcement provisions are severe. HIPAA imposes civil penalties enforced by the Office of Civil Rights, of $100 per violation with up to $25,000 for all violations of a single standard per year. HIPAA also contains criminal penalties that will be enforced by the Department of Justice. Violations made "knowingly" may be enforced with fines up to $50,000 and/or up to one year in prison. Offences occurring under "false pretenses" may be enforced with fines up to $100,000 and/or up to five years in prison. Violations committed with the intent to sell, transfer, or use health information for commercial advantage, personal gain, or malicious harm can incur fines up to $250,000 and/or up to ten years in prison.