HIPAA SUMMARY

WHAT IS HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established certain standards and procedures regarding health information data to further two goals:

- improving the accessibility of personal health information; and
- protecting patients' right to the privacy of their health information.

While HIPAA includes provisions intended to improve the portability of health coverage, the ACA's insurance protections have for the most part superseded HIPAA's rules. This summary focuses on HIPAA's privacy, security and breach notification rules.

WHO IS COVERED BY HIPAA

The reach of HIPAA is often misunderstood. As originally passed, HIPAA named three "covered entities," (i.e., individuals or entities subject to HIPAA):

- Healthcare providers;
- Health Plans;
- Healthcare clearing houses.

HIPAA has since been amended to include "business associates" of health plans as covered entities. A business associate is simply a vendor that assists a health plan, i.e., an insurance broker or consultant, a TPA, a pharmacy benefit manager, etc.

Contrary to popular understanding, employers are **not** directly subject to HIPAA. An employer is only subject to HIPAA when it is acting on behalf of the employer's group health plan. For example, in processing an employee FMLA request, an employer obtains personal health information from an employee regarding his/her request. HIPAA does not apply to the FMLA health information obtained by the employer. In processing the FMLA claim, the employer is acting as an employer, not as a health plan sponsor, and the information came from the employee, not from the health plan. (That doesn't mean that the information is not protected and subject to certain privacy requirements; FMLA, the ADA and other provisions also protect health information.) Similarly, employers often obtain significant health information in connection with workers compensation claims. Again, however, workers compensation claim information does not come through the health plan, but rather comes to the company in its role as an employer. The same is true if an employee tells an employer about his/her health condition in connection with an absence from work, or just as part of conversation. The information did not come from the health plan, or come to the employer in its capacity as a plan sponsor, so is not subject to HIPAA.

On the other hand, when an employer receives health plan information that constitutes personal health information (think large claim reports or any other plan reports that contain information about a plan participant's health, medical treatment or payment for medical treatment), HIPAA applies. Similarly, if an employer assists an employee with a claim under the health plan, the health information learned in the process is subject to HIPAA.

WHAT INFORMATION IS COVERED BY HIPAA

HIPAA covers “protected health information” or “PHI”. PHI is health information that is individually identifiable. Information that is aggregated or de-identified so that it cannot be tied to an individual is not subject to the HIPAA rules.

HIPAA PRIVACY RULE

The HIPAA privacy rule sets out various rules or standards that govern when a covered entity can use or disclose PHI. As a general rule, a covered entity can always use or disclose PHI either internally or to another HIPAA covered entity where such use or disclosure is for treatment, payment or health care operations purposes. However, any such use or disclosure must be the minimum necessary to accomplish the allowed task. The HIPAA privacy rule provides additional specific standards for other situations in which PHI can be used or disclosed for certain purposes, or when the patient’s consent must be obtained. HIPAA also has other procedural rules for covered entities that address required written policies, training, and record and document retention. Fully insured plans that do not see any PHI qualify for an exemption (the “hands off” exemption) from most of the HIPAA privacy rules.

HIPAA SECURITY RULE

The HIPAA security rule sets certain standards that covered entities generating, maintaining or using electronic PHI (“ePHI”) must meet to ensure the security of the electronic data. Covered entities are only subject to the security rule if they have access to ePHI. Some employers avoid access to ePHI so that the security rules do not apply. In general, the security rules address certain administrative, physical and technical safeguards that must be maintained by the covered entity to ensure the security of ePHI. A covered entity subject to the Security Rule must conduct a security risk analysis that considers the type of ePHI accessed by the organization, risks to that ePHI and the safeguards that should be implemented to protect ePHI. (Note: Fully insured plans that qualify to for the Hands Off exemption are also not subject to HIPAA’s security rule.)

BREACH NOTIFICATION

The breach notification rule requires those covered under HIPAA to advise patients when a security breach of their unsecured health information has occurred.

WHO ENFORCES HIPAA?

The Department of Health and Human Services, Office for Civil Rights (OCR), enforces these rules and regulations. OCR conducts complaint investigations and will administer periodic compliance audits.

Non-compliance can be subject to a number of hefty punishments. Monetary penalties can be imposed on all entities that fail to adhere to HIPAA rules and regulations. Specifically, an entity that violates the HIPAA can be subject to monetary penalties of $50,000 or more per violation. Entities that knowingly violate HIPAA can also be subject to criminal penalties.