HIPAA Privacy

The HIPAA Privacy Rule establishes safeguards and procedures to regulate the use, disclosure, and privacy of an individual’s health information. HIPAA privacy is of particular concern to employers now, as the U.S. Department of Health and Human Services Office of Civil Rights has launched a HIPAA Phase 2 Audit Program. This brief summarizes the core concepts and requirements of the HIPAA Privacy Rule, and describes differences in how the privacy requirements apply to self-funded health plans and fully insured health plans.

Generally self-funded and level funded health plans must comply with the core privacy requirements. Fully insured plans may be exempt from or have limited responsibility for complying with some of the core privacy requirements. This is particularly the case for fully insured plans operated without access to PHI (so called “hands off” plans). A plan that is totally hands-off and receives only aggregated or summary health information should still comply with the privacy prohibitions against intimidating or retaliatory acts and against requiring a waiver of HIPAA rights. In addition, self-funded, self-administered health plans with fewer than 50 participants are exempt from the HIPAA privacy rules. This exemption rarely applies other than for some HRAs or health FSAs which are 100% employer self-administered.

Core Concepts

The following are common basic terms necessary for understanding the HIPAA privacy requirements:

- “Individually Identifiable Health Information” is health information that is created or received by a health care provider, health plan or health clearing house.
- “Protected Health Information” (PHI) is “individually identifiable health information” that is maintained or transmitted by a “covered entity if it relates to the past, present, or future physical or mental health condition, treatment, or payment for treatment, with respect to an individual, and identifies the individual or could reasonably lead to the identification of the individual. Common examples of PHI are claims information and plan enrollment and disenrollment information (e.g. lists of plan participants). PHI does not include information such as health information maintained in an employer’s employment records, or de-identified information such as aggregate claims data.
- “Covered Entities” include health plans, health care clearinghouses, and health care providers. This brief focusses on covered entities that are employer-sponsored group health plans. For purposes of the HIPAA privacy requirements, a group health plan includes employer medical plans, health reimbursement arrangements (HRAs), health FSAs and, potentially, dental and vision plans if not deemed excepted benefits.
- “Business Associates” are persons or entities that on behalf of a health plan or other covered entity create, receive, maintain, or transmit PHI. The covered entity’s workforce is not a business associate. Business associates may include insurance brokers, third-party administrators (TPAs), attorneys, accountants, or other persons or entities that receive PHI from your health plans.

Core Requirements

The following are some important requirements of the HIPAA Privacy Rule that employers should be aware of in order to protect the privacy of health plan PHI:

- Permitted Use and Disclosure of PHI. As a covered entity, an employer’s health plan can use and disclose PHI for purposes of treatment, payment, and health care operations, which includes many routine operations of a health plan. Any use or disclosure that is not for a permitted use will generally require written authorization from the individual to whom the PHI relates. For example, an employer may not disclose PHI from the health plan for life insurance, disability insurance or for purposes of a workers’
compensation claim as its' not a permitted use, and would require a written authorization from the individual. Another non-permitted use is a covered entity disclosing PHI to a family member without written authorization from the individual. Generally, with a written authorization, a covered entity may use and disclose PHI for any purpose specified in the authorization, except that genetic information cannot be used or disclosed for underwriting purposes.

- Minimum Necessary Standard. When the use, disclosure, or request of PHI is permissible, covered entities and business associates must use, disclose, or request only the “minimum necessary” PHI to accomplish the intended purpose. The HIPAA privacy regulations specifically state that disclosure of an entire medical record is presumed to violate the minimum necessary standard.

- Health Plan “Firewall.” To safeguard the privacy of PHI, an employer must reasonably segregate the operations of the health plan from other employer operations – creating a sort of “firewall” separating health plan operations (the “covered entity”) from the remainder of the employer’s personnel and operations. The persons working inside the “firewall” are the workforce members. Creation of this “firewall” on behalf of the covered entity requires (1) identification of the persons or group of persons within the workforce who need access to PHI to carry out their duties, and (2) taking precautions to ensure that only those persons have access to PHI. Written documentation may also be required.

- Physical Safeguards. Physical safeguards may be necessary to prevent disclosure of PHI. These may include keeping PHI in locked rooms or file cabinets or computers, with keys or passcodes only accessible by authorized health plan personnel, not keeping PHI in the same files as other employee HR information, and shredding documents containing PHI prior to disposal.

- HIPAA Privacy Policies and Procedures. Most covered entities must have written HIPAA privacy policies and procedures with respect to the use, disclosure, and safeguarding of PHI. This includes designation of a privacy official who is responsible for development and implementation of the covered entity’s privacy policies and procedures, and to answer questions or complaints regarding the HIPAA privacy rules. All personnel within the firewall must be trained regarding the covered entity’s HIPAA privacy policies and procedures. Training for each individual must be documented, a refresher provided periodically, and may need to be updated based on regulatory changes or internal practices.

- Business Associate Agreements. Covered entities must determine who are their business associates and have signed HIPAA-compliant business associate agreements with all business associates who may receive or otherwise have access to PHI on behalf of the covered entity. The business associate agreement should be executed prior to the sharing of any PHI.

- Notice of Privacy Practices. Many covered entities must distribute to employees of the plan sponsor a notice describing the uses and disclosures of PHI that may be made by the covered entity, the individual’s rights regarding their PHI, and the covered entity’s duties with respect to safeguarding the privacy of PHI. Individual rights include the right to inspect and copy his or her PHI, the right to request amendments to inaccurate or incomplete PHI, the right to request an accounting of the disclosures of PHI, and the right to request restrictions on PHI use and disclosure. The U.S. Department of Health and Human Services has issued a model notice to assist covered entities with designing a HIPAA notice of privacy practices.

For most employers with health plans that create, maintain, transmit or receive PHI, an awareness of the requirements of the HIPAA privacy rules is extremely important. With audits by the federal government ramping up, and the penalties or damages having been increased for noncompliance, it is worthwhile for employers to engage legal counsel for a HIPAA compliance review of their health plan documentation and operations.

The information contained herein is for general informational purposes only and does not constitute legal or tax advice regarding any specific situation. Any statements made are based solely on our experience as consultants. Marsh & McLennan Agency LLC shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein.