EMPLOYER
LEGAL BRIEF

MARCH 2012 Published by Personnel Concepts

Complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations issued by the U.S. Department of Health and Human Services ("HHS") generally limit how entities may use and disclose individuals' medical information and increase individuals' control over the privacy of and their access to this information.

HIPAA is divided into several sections, including the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") and the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule"). The Health Information Technology for Economic and Clinical Health ("HITECH") Act amended HIPAA to address concerns associated with the electronic transmission of health information. HHS, through its Office for Civil Rights, investigates complaints, conducts compliance audits, and may refer possible criminal violations of HIPAA to the US Department of Justice. HITECH strengthened HHS's civil and criminal enforcement of HIPAA by increasing potential penalties and the circumstances under which HHS may seek penalties.

The HHS has issued two regulations applicable to entities covered by HIPAA

The HHS has issued two regulations, "Standards for Privacy of Individually Identifiable Health Information" and "Health Insurance Reform: Security Standards" applicable to entities covered by HIPAA. The new regulations will guide the implementation and enforcement of the provisions passed by Congress in the HITECH Act of 2009 as part of the American Recovery and Reinvestment Act that add new protections to the regulations from the original 1996 HIPAA authority. The new regulations will improve patient privacy and security protections by extending the Office for Civil Rights' enforcement to business associates and covered entities, strengthening individuals' rights to request and receive their medical information in electronic form, and setting new limits on the use and sale of individuals' information.

The HHS Secretary Kathleen Sebelius said that the new rules and resources will strengthen the privacy of health information and to help all Americans understand their rights and the resources available to safeguard their personal health data. HHS is working with public and private partners to ensure that, as the use of health information technology to drive improvements in the quality and effectiveness of our nation's health care system is expanded, Americans can trust that their health information is protected and secure.

In preparation for the finalization of the regulations, employers are encouraged to review their policies and practices under existing rules, as well as take steps to decrease exposure of covered protected health information (PHI). The following is an overview of some of the more significant provisions of HIPAA impacting small and mid-size businesses and health plans.

I. What information is protected?

The Privacy and Security Rules protect health information that can be used to identify an individual (for example, name, address, birth date or Social Security number) and that pertains to an individual's past, present or future physical or mental health; the provision of health care to the individual; or the past, present, or future payment for health care, all referred to as PHI. If data is so limited that it cannot be linked to any particular individual, the Rules do not apply to that data.

The Security Rule has slightly narrower coverage than the Privacy Rule, and protects only PHI in electronic form, referred to as "electronic protected health information" ("e-PHI"). The Privacy Rule, on the other hand, applies to all PHI, whether it is transmitted electronically, orally or in writing.

II. Who must comply?

Most provisions of HIPAA govern individuals and entities that are "covered entities," which include individual and company group health plans, health care providers, health insurance companies, HMOs, and health care clearinghouses. While employer-sponsored group health plans are "covered entities" subject to the Rules, those group health plans with less than 50 participants that are administered solely by the

employer that maintains the plan are exempt from coverage.

Some businesses that do not fall within the definition of "covered entity" are, nonetheless, affected by the Privacy and Security Rules and should be aware of how HIPAA may impact their business operations. When a covered entity uses a service provider to perform legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services, and the service provider has access to PHI, the covered entity must include certain protections for medical information in a Business Associate Agreement between the covered entity and the service provider. Typical business associates include claims processors, data analysts and billing services.

The Business Associate Agreement should describe the permitted and required uses of PHI by the business associate, provide that the business associate will not use or further disclose the PHI other than as permitted or required by the agreement or as required by law, and require the business associate to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the agreement.

III. Privacy of Health Information

The Privacy Rule aims to protect health information by establishing national standards (1) addressing how PHI may be used and disclosed by covered entities, and (2) for individuals' privacy rights so individuals can better understand and control how their health information is used. When a covered entity has a permissible reason to use, disclose or request PHI, it must use reasonable efforts to limit this use, disclosure or request to only the minimum amount of information needed to accomplish the intended purpose.

Fully-insured group health plans – those providing benefits solely through insurance or HMO contracts – that receive only enrollment data and certain summary health information are exempt from most of the Privacy Rule's requirements. The only administrative obligations with which these plans are required to comply are a ban on retaliatory acts and waiver of individual rights, and certain documentation requirements if plan documents are amended to provide for the disclosure of PHI to the employer plan sponsor. These employers should be careful to maintain the exemptions afforded them from most provisions of the Privacy Rule when their employees assist plan participants with health insurance questions because the employees may be in a position to receive more PHI than simply enrollment data and summary health information.

A. Permitted Uses and Disclosures of Health Information

The Privacy Rule permits a covered entity to use and disclose PHI, without first getting an individual's authorization, in limited circumstances, including the following: (1) to provide the PHI to the individual who is the subject of the information; (2) for treatment, payment, and health care operations for the individual; (3) where the individual is incapacitated, in an emergency situation, or not available, if the use or disclosure is in the best interests of the individual; and (4) when the use or disclosure is required by law, as for example, in response to a court order or to provide information to law enforcement officials under certain circumstances.

B. Uses and Disclosures Requiring Individual's Written Authorization

A covered entity must obtain an individual's written authorization for any use or disclosure of PHI that is not otherwise permitted by the Privacy Rule, and a covered entity may not condition treatment, payment, enrollment or benefits eligibility on an individual granting an authorization, except in limited circumstances.

In most cases, authorization is required to use PHI for marketing purposes, whether the marketing is geared toward the public or to another entity. PHI may be used, however, in certain situations, such as to send communications to health benefit plan enrollees about participating providers, replacement of or enhancements to the plan, and health-related products or services available only to plan enrollees.

All authorizations must be in plain language and contain the following, among other data: the information to be disclosed or used and the person(s) disclosing and receiving the information; when the authorization expires, by expiration date or event (for example, "upon termination of enrollment in the health plan"); and the right to revoke the authorization in writing.

C. Individuals' Right to Access and Correct PHI

Generally, individuals have the right to obtain copies of and review their PHI in covered entities' records. Only certain

EMPLOYER COMPLIANCE TIPS

1. Make sure that you and your staff are aware of HIPAA Privacy and Security requirements and understand how they apply to your business.
2. Assess all the information system components that interact with protected health information at your worksite.
3. Implement procedures that utilize administrative, physical and technical safeguards to protect covered PHI.
4. Have procedures in place for addressing a breach should one occur.◆

PHI, such as psychotherapy notes and information compiled for legal proceedings, may be withheld, and then only under certain circumstances. Covered entities may charge the individual for the cost of copying the records and for postage.

The Privacy Rule also gives individuals the right to have covered entities amend their PHI when that information is inaccurate or incomplete, and sets out processes and notification requirements when covered entities grant or deny change requests.

D. Privacy Policies and Procedures

The Privacy Rule also requires that a covered entity designate persons or offices for certain functions, including to develop privacy policies and procedures, and to act as a contact for receiving complaints and questions about privacy practices. A covered entity must train all workforce members on its privacy policies and procedures and sanction those who violate them.

A covered entity must also develop and maintain a privacy notice that includes, among other information, the covered entity's duties to protect privacy, an explanation of its privacy practices, a description of individuals' rights if they believe their privacy rights have been violated, and the point of contact for making complaints to the covered entity.

Each covered entity must provide a copy of its privacy notice to any person who asks for it, and post the notice on its Web site. Health plans in particular must also (1) provide the notice to individuals when they enroll in the plan, (2) provide a revised notice to plan participants within 60 days of a material revision to the notice, and (3) at least once every three years, notify participants of the availability of and how to obtain a copy of the privacy notice. The Rule also sets forth specific notice distribution requirements for direct treatment providers.

E. Self-funded Health Plans

Those with self-funded health plans should be aware of additional requirements specific to them. If the employer plan sponsor has access to the PHI of the plan participants, the sponsor must certify that it has amended the plan documents to ensure that the PHI will be used only for plan administration functions. The amendments must specify the particular administrative functions to be performed by the sponsor on behalf of the plan, prohibit the use of PHI for employment-related functions, and contain other statements set forth in the Privacy Rule.

The amended plan documents must create a "firewall" so only employees within the firewall have access to PHI. The employer must (1) communicate to plan participants the identity of those employees inside the firewall, and (2) train supervisors and others outside the firewall to re-route health plan questions to employees inside the firewall.

As with other covered entities, the employer must have in place business associate agreements with all its business associates, including those used in connection with the self-funded plan.

IV. Securing Health Information

Both the Privacy Rule and the Security Rule require that entities implement administrative, physical and technical safeguards to protect the confidentiality of PHI and prevent unauthorized access to PHI. Entities may comply with the Privacy Rule (which applies to PHI in electronic, oral or paper form) for example, by shredding documents containing PHI before discarding them or securing medical records with lock and key.

The Security Rule, which applies to ePHI (electronic), requires use of certain information technology standards and best practices in regard to issues such as network security, data encryption, protection from malicious software, securing PHI in the cloud and disposing of ePHI. The Rule is broken down into standards that must be met, and "implementation specifications," which are detailed instructions, either mandatory or optional, on how entities can comply with each standard. The Federal Trade Commission and the National Institute of Standards and Technology provide helpful information on how to implement safeguards, but given the highly technical aspect of the Security Rule, smaller entities often need to consult health information technology ("HIT") resources to help them to comply with the standards.

The Security Rule also imposes organizational requirements (for example, facility access controls and security awareness and training) analogous to the Privacy Rule.

The basic process that a covered entity must follow to comply with the Security Rule is as follows: identify its current security measures and risks; develop an implementation plan after reviewing the standards and implementation specifications; implement solutions appropriate for the organization; document its decisions, analysis and rationale for its decisions; and periodically reassess and update its security measures and documentation in response to any changes that affect the security of its ePHI. While compliance with the standards is mandatory, they are intended to be flexible so that an entity may take into account its size and resources and the costs when deciding which security measures to utilize to meet the standards.

V. Other Notable Requirements Under HIPAA

A. Breach Notification

Incidents that put the confidentiality of PHI at risk occur quite frequently, and commonly involve the theft or loss of laptops, smartphones, flash drives, network servers or other devices that house PHI; improper disposal of paper documents

containing PHI by business associates, especially third party billing services; hacking incidents; and misdirected mail. A security breach under the Privacy Rule is generally an impermissible use or disclosure that compromises the security or privacy of PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual(s).

Following a breach of "unsecured PHI," HIPAA, as amended by the HITECH Act, requires that covered entities and their business associates notify the affected individuals, HHS, and, in certain circumstances, the media. The notification to individuals must be provided without unreasonable delay and in no case later than 60 days following discovery of a breach. Note that similar breach notification provisions implemented and enforced by the Federal Trade Commission apply to vendors of personal health records and their third-party service providers.

Covered entities and business associates need to provide the required notifications only if the breach involved unsecured PHI. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS in guidance published in the Federal Register on April 27, 2009 at 74 Fed. Reg. 19006.

B. Health Insurance Portability

HIPAA also addresses health coverage portability when an individual changes jobs. Some employment-based group health plans limit or deny coverage for preexisting conditions. HIPAA generally limits which types of conditions can be subject to a preexisting condition exclusion, sets a maximum preexisting condition exclusion period, and allows individuals to receive credit for recent prior health coverage, reducing the time they can be excluded from a new employer's health plan for a preexisting condition.

C. Discrimination

HIPAA also provides that individuals may not be denied eligibility or continued eligibility to enroll in a group health plan based on any health factors, and may not be charged more than any similarly-situated individual based on health status, medical condition, claims experience, receipt of health care, medical history, genetic information, evidence of insurability or disability.

VI. Upcoming Changes to HIPAA Rules

HHS has issued a number of proposed regulations that, if adopted in final form, would require that employers revise their procedures for responding to breaches and information requests, business associate agreements and HIPAA privacy notices. In a recent notice published in the Federal Register, HHS said they aim to issue final regulations in March 2012. Watch for the following rules:

In mid-2010, HHS published proposed regulations that would extensively modify the HIPAA rules as required under the HITECH Act. Changes would include making more HIPAA requirements directly applicable to business associates, expanding individuals' rights to obtain restrictions on certain disclosures of PHI to health plans, and exposing covered entities and business associates to greater liability risk for violations.

In 2011, HHS issued a proposed rule that would give individuals the right to obtain a report on who has accessed their ePHI. Although covered entities are currently required to track access to ePHI, they are not required to share this information.

HHS has also proposed broadening the breach notification requirement currently in effect to address a point of controversy – to require that entities must report all breaches, not only those breaches that entities determine pose a significant risk of harm to affected individuals.

Businesses should watch for the coming final rules and seek guidance on how to comply by the effective dates or any delayed compliance dates. ◆

Gina A. Haschke *is the founding partner at Haschke Law PLLC and practices in the areas of privacy, e-commerce and intellectual property law. She earned her Juris Doctorate degree from Southern Methodist University Dedman School of Law in Dallas, Texas in 2003 and holds bar licenses in Washington, DC and Texas. Before opening her own practice, she worked in law firms, most recently in the Washington, DC office of a major international law firm. Ms. Haschke has worked with startups and Fortune 500 companies, and has represented clients before federal and state regulators. For more information, you may contact Ms. Haschke at 214-431-5110 or ginahaschke@haschkelaw.com.*

EMPLOYER
LEGAL BRIEF

Published by Personnel Concepts
3200 E. Guasti Road, Suite 300, Ontario, CA 91761
www.personnelconcepts.com
E-mail: answers@personnelconcepts.com

Managing Editor: Kim Cabanting
Editor: Gary McCarty
Graphic Artist: Lorraine Maschler