*Source: International Society of Certified Employee Benefit Specialists

HIPAA's Privacy Rule:

What Is It, and How Does It Affect You?

by Melinda Balezentis

and Steve Halterman, CEBS

►This article discusses the implications for stakeholders of the privacy rule under the Health Insurance Portability and Accountability Act of 1996, on which the U.S. Department of Health and Human Services first released guidance on July 6, 2001. *Although guidance will continue to evolve, the authors urge organizations to initiate the implementation of policies to ensure compliance by the actual effective date of 2003. (Small health plans have until 2004 to comply.)*◄

Since its inception more than five years ago, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) has had a significant impact on those who provide or utilize health insurance benefits. Until now, most if not all of this impact has come from the "portability" provision, which has significantly changed the way insurers treat preexisting conditions for new enrollees. Prior to the enactment of HIPAA, changing health plans could be a financially devastating event for individuals with ongoing medical conditions. Because of HIPAA, individuals are now free to change employers, and health plans, without risk of coverage limitations because of preexisting conditions.

THE BROAD SCOPE OF HIPAA

Although portability was a major breakthrough in providing access to health care coverage, there is actually much more to HIPAA. The legislation was a compilation of many separate issues that had been on the legislative agenda for several years. The final version of HIPAA as it was enacted accomplished the following:

- Authorized the pilot program for medical savings accounts (MSAs)
- Created a Medicare fraud control program
- Established parity for mental health benefits
- Revised the tax deductibility of corporate-owned life insurance (COLI)
- Created favorable tax provisions for long-term care insurance
- Established favorable tax treatment for accelerated death benefits
- Allowed for greater access to and portability of health care coverage and
- Provided for administrative simplification in health care data interchange.

Although many of HIPAA's rules became effective in 1996 and 1997, several have yet to take effect. One of the more emotionally charged rules contained within the legislation is the so-called privacy rule. The privacy rule was set forth through the administrative simplification provision of the act, which encompasses the following:

- Electronic health care transactions (final rule issued)
- Medical privacy (final rule issued)

- Security requirements (proposed rule issued; final rule in development)
- Unique identifier for employers (proposed rule issued; final rule in development)
- Unique identifier for providers (proposed rule issued; final rule in development)
- Unique identifier for health plans (proposed rule in development) and
- Enforcement procedures (proposed rule in development).

"An important aspect of the privacy rule is that significant penalties have been established for misuse of personal health information."

THE HIPAA PRIVACY RULE

HIPAA directed Congress to pass privacy legislation by August 21, 1999. When Congress failed to do so, responsibility for developing the regulation fell to the U.S. Department of Health and Human Services (HHS).

HHS developed the proposed rule in November 1999 and, after receiving more than 50,000 comments from the public, published the final rule on December 28, 2000. It became law on April 14, 2001, but the actual effective date for covered entities to be in compliance is April 14, 2003. Small health plans (with annual receipts of $5 million or less) have until April 14, 2004 to comply.

The privacy rule is intended to protect the confidentiality of an individual's health information. It requires organizations that collect or access health information in order to provide care or process information about that care to implement and enforce specific safeguards and consent procedures. Not only is the information protected, but individuals also must be given access to their information in order to validate its accuracy.

An important aspect of the privacy rule is that significant penalties have been established for misuse of personal health information. Not only are there civil penalties, but Congress also has established steep criminal penalties for those who knowingly violate patient privacy. The penalties range from one year in prison and $50,000 for obtaining or disclosing protected health information, to up to ten years in prison and $250,000 for obtaining or disclosing such information with the intent to sell it or use it for personal or commercial advantage or malicious harm. As patient privacy has become a serious issue in this age of electronic information processing, the government has made it clear that violators will be prosecuted to the full extent of the law.

Key Terms

It is important to understand the key terms associated with the HIPAA privacy rule. These terms are defined below.

- *Covered entities* are the entities that must comply with the privacy rule. These are health plans, health care clearinghouses and health care providers that conduct certain financial and administrative transactions electronically.
- A *business associate* is a person or entity that provides certain functions, activities or services for or to a covered entity involving the use and/or disclosure of protected health information, or PHI.
- *TPO* refers to treatment, payment or health care operations.
- *Protected health information (PHI)* refers to all medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper or orally; all are covered by the final rule.
- *Individually identifiable health information* is health information (including demographics) created or received by a covered entity (health care provider, health plan, employer or health care clearinghouse) that relates to the past, present and/or future physical or mental health condition of

an individual that can or may be used to identify the individual.

- A *health plan* is an individual or group health plan, a health insurance issuer, certain long-term care insurance issuers and Medicare, Medicaid and other government-based health insurance programs.
- *Health care* refers to care, services or supplies related to the health of an individual. This includes but is not limited to: preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care and counseling; a service, assessment or procedure with respect to an individual's physical or mental condition or functional status or that affects the structure or function of the body; and the dispensing of a drug, device, equipment or other item in accordance with prescription.
- *Health care clearinghouses* are public or private entities (including billing services, repricing companies, community health management information systems or community health information systems) and "value-added" networks and switches that process health information.
- *Consent* refers to a general document that gives health care providers that have a direct relationship with the patient permission to use and disclose all PHI for TPO.
- *Authorization* refers to a more customized document that gives covered entities permission to use specified PHI for specific purposes that are generally other than TPO, or to disclose PHI to a third party specified by the individual.

WHO ARE THE STAKEHOLDERS?

In addition to the covered entities (health plans, health care clearinghouses and health care providers), patients (employees and their dependents), employers and vendors (such as medical management organizations and consultants) are greatly affected by the privacy rule. The following provides an outline as to how each organization is affected and what courses of action need to be taken toward compliance.

Health Plans

As covered entities, health plans will be required to comply with HIPAA rules and specific state legislative initiatives focused around the use of individual health information. Health plans generally provide coverage either on an insured or self-insured basis. Each of these has unique compliance requirements under HIPAA. In an insured offering, the insurer or health plan assumes the total risk for paying claims. The health plan will collect data on participants through the process of paying claims and will use this information to estimate the future type and cost of medical services consumed by any given employer group. This detailed information is used to estimate how much the health plan will adjust the premium rates for the following contract period.

"HIPAA creates a new challenge for health plans that operate with subcontracted vendors, as these entities have not routinely been identified in the employer group contract."

Many health plans "carve out" or subcontract with organizations that provide medical or case management services. The purpose of these types of carve-outs is to maximize any cost savings by identifying and coordinating services in the most cost-efficient manner. These third-party entities hold a contract with the health plan but not the employer. It is imperative for these entities to have access to individual claims data to deliver the contracted services.

HIPAA creates a new challenge for health plans that operate with subcontracted vendors, as these entities have not routinely been identified in the employer group contract. HIPAA will require full disclosure of these entities, their purpose and what information will be provided to them. It is anticipated that all health plans will have to implement privacy

"In general, health care providers who see patients will be required to obtain consent before sharing information for treatment, payment and health care operations (TPO)."

policies that comply with the applicable provisions of HIPAA and include these in all member materials.

In a self-funded environment, health plans have similar responsibilities for compliance with the addition of detail data transfers to "carved out" service vendors directly contracted with an employer. Under HIPAA this presents a new challenge for health plans. Health plans are reluctant to share the data they collect through claims processing or disease case management to a third party with whom they do not have a contractual arrangement. This reluctance stems from a threat of fines and/or penalties if the proper safeguards are not present in the operations of the third-party vendor. This can present a problem for an employer offering employee benefits with multiple "carved out" services dependent upon carrier information for program viability.

Health plans and insurance carriers that act as a TPA and prepare the summary plan documents will have to comply with the requirement to include specific HIPAA-approved language detailing the rights and responsibilities of all participating parties. There is a strong probability that additional rules or interpretation of existing rules will surface as we move closer to the compliance dates for initial implementation of the privacy standards. A health plan not categorized as "small" must comply with the applicable requirements no later than April 14, 2003. Small health plans have until April 14, 2004.

Health Care Providers

Health care providers have, by far, the most visible responsibilities for privacy rule compliance. The main entities categorized as "providers" are hospitals, medical practices and pharmacies.

Hospitals and Medical Practices

Hospitals and medical practices will be required to provide information to patients about their privacy rights, adopt clear privacy procedures, train employees so they understand the procedures, designate a privacy official and secure patient records so they cannot be accessed by those who do not need the information.

The privacy rule gives flexibility to providers, as the rules are scalable to the size of the organization. In a large hospital, the privacy officer may be a full-time dedicated position, perhaps even with a staff that reports to the privacy officer, while the small physician practice may simply designate the office manager or receptionist to handle the privacy officer responsibilities. Additionally, the policies and procedures of small practices may be more limited under the rule than those of a large hospital. This will be based upon the actual volume of health information transactions.

In general, health care providers who see patients will be required to obtain consent before sharing information for treatment, payment and health care operations (TPO). Additionally, separate patient authorization must be obtained for nonroutine disclosures and most nonhealth care purposes. Patients will have the right to restrict the use of these disclosures.

As the privacy rule is meant to *help* patients and not limit their access to quality health care, there are circumstances in which consent does not have to be obtained, such as emergency situations. In the case of an emergency, the provider does not have to obtain consent until the situation allows for reasonable communication with the patient. This is meant to give providers discretion so that care is not delayed.

Within the HHS guidance, there are several confusing issues that have since been clarified in order to ease the perceived burden placed on providers. One section makes it clear that hospitals do not have to take such steps as building

soundproof rooms so that conversations about PHI are not overheard. Rather, the guidance states that reasonable safeguards need to be provided, such as curtains, screens and similar barriers.

Pharmacies

Pharmacists as health care providers will be required to obtain consent as well. However, through the HHS guidance, clarification has been made to ensure that undue restrictions will not be placed on pharmacy operations. For example, friends and relatives will be able to pick up prescriptions, and physicians may phone in prescriptions before the pharmacist obtains consent.

Patients

Patients are the intended beneficiaries of the privacy rule. They will have the responsibility to be aware of their privacy rights and to report any potential violations. Generally, patients will be required to sign consent forms prior to receiving care or discussing their individual health information with providers. Additionally, individuals will be required to sign authorization statements when enrolling in health plans. It is the individual's responsibility to read and understand these statements prior to giving authorization. Individuals have the right to revoke authorization or consent at any time.

Employers

Although employers are not considered covered entities under the privacy rule, they certainly have a great deal at stake with its compliance. The actual level of involvement will depend upon each employer's funding and administrative vehicle utilized for health coverage. Employers that self-fund their health benefits will be required to do more than employers with fully insured plans. Further, employers that self-administer (pay claims in-house) will have even greater responsibility. In fact, because the self-administered employer is acting in a health plan capacity, it will actually become a "covered entity" and will have to comply with the same rules as a health plan.

All employers, regardless of funding and administrative vehicles, will be required to develop formal privacy policies and amend their plan documents to reflect those policies. Without implementing these policies, health plans will be prevented from sharing any PHI with the employer. Here is a brief summary of the responsibilities of each of the employer categories.

Employers With Fully Insured Health Plans

Employers with fully insured health plans must amend their plan documents to describe the health plan's health information privacy policies.

The policy must provide that the employer agrees to follow various rules, such as: not using or disclosing PHI other than as permitted by law; ensuring that business associates will follow such rules; making plan participants' PHI available to them upon request; returning or destroying all PHI when it is no longer needed; identifying who will have access to PHI; and establishing a mechanism for resolving noncompliance issues.

The fully insured employer will have no additional responsibilities for compliance with the privacy rule if the employer limits its plan administration functions to the following two basic functions: eligibility and enrollment determinations; and receipt of only summary health claims information (without identifying individual employees).

Employers That Self-Fund Health Benefits: TPA as the Claims Administrator

In addition to amending the plan documents as described above, the self-funded employer must create a privacy administration infrastructure, which will support the protection of individual health information in accordance with the privacy rule.

The Authors

Melinda Balezentis, M.S., and **Steve Halterman, CEBS,** are health care consultants with William M. Mercer, Incorporated in Houston, Texas, where they have been conducting employer forums and are preparing privacy rule compliance readiness programs for employers. Ms. Balezentis' experience is in health plan and TPA operations and vendor management. She earned her B.S. degree in biomedical science from Texas A&M University and her M.S. in health care administration from Texas Woman's University. Mr. Halterman's experience is in group benefit plan design, financing and vendor management. He earned his B.A. degree in business communication from Baruch College, City University of New York.

"When an employer is self-administering its employee welfare benefits plan, it is actually performing several basic 'health plan' functions."

This privacy administration infrastructure should designate a privacy official, provide notices of information practices to plan participants, provide privacy training, implement safeguards to protect information from misuse, provide a vehicle for complaints about violations, and develop a system of sanctions for employees and business associates who violate the policies.

Employer as the Claims Administrator

When an employer is self-administering its employee welfare benefits plan, it is actually performing several basic "health plan" functions. Again, this causes the employer to become a "covered entity" that is responsible for complying with all the same rules as a health plan. Additionally, the employer will be responsible for implementing all of the required compliance standards listed above. The employer will also be required to provide written notice of health information practices, provide access to an individual's PHI, and establish a process for the individual to request amendment or correction of PHI that is inaccurate or incomplete.

Contracted Components of Health Plans (Carve-Outs)

Carve-outs would encompass all specialty vendors involved with a health plan, to include:

- Utilization management/review
- Disease management
- Mental health vendor
- Employee assistance program (EAP)
- Health promotion organization
- Nurse advice line (24-hour).

These organizations are considered "business associates" of a health plan and are considered covered entities because they enter into a health care arrangement where the provision of services rendered involves access and/or disclosure of individually identifiable health information. These entities generally contract with medical carriers to provide specialty services. They can contract with employers if the benefits are offered through a self-funded arrangement. The health plan delegates authority to these vendors for daily operational activities with the caveat that each is expected to have the appropriate safeguards in place to prevent the use or disclosure of information other than as provided for by the contract with the health plan or employer.

Consultants

Since consultants are considered "business associates," they will be required to comply with the privacy rule. However, business associates are only indirectly regulated. Employers should have consultants agree to the same terms as any other business associate. It is the employer's responsibility to ensure that all business associates comply with the privacy rule as if they were a covered entity.

CHANGES TO THE FINAL RULE

Although it is called the "final" rule, the rule is not final at all. On July 6, 2001, after receiving more than 7,000 comments from the public, HHS issued its first guidance on the privacy rule, the first of many revisions. More recently, HHS conducted a public meeting in order to hear further comments on the implications of the privacy rule. Based on this input, HHS intends to incorporate more changes and issue further guidance in order to help meet the needs of those who will be affected by the rule. According to HHS, the intent is to simplify compliance requirements so as to not adversely affect patients' access to quality health care.

Some of the proposed changes announced through the July 6 guidance include:

- *Phoned-in prescriptions*—Pharmacists will be permitted to fill prescriptions phoned in

by the patient's doctor before obtaining written consent from the patient.

- *Referral appointments*—Providers will be permitted to schedule appointments, surgery and other procedures prior to obtaining written consent from the patient.
- *Allowable communications*—Wording will be revised in order to increase the confidence of covered entities. The purpose is to ensure that providers are free to engage in effective, quick communications for quality health care. This will include oral communications with family members and treatment discussions with staff involved with the coordination of patient care.
- *Minimum necessary scope*—This will clarify that certain common practices, such as sign-in sheets, X-ray lightboards and bedside medical chart utilization, will be allowable.
- *Parental access*—A revision may be made to give parents appropriate access to health information about their children.

Therefore, as the rule is still undergoing changes, it will be important to understand the implications for each of the covered entities and others affected by the privacy rule. By the time this article is published, there will undoubtedly be new revisions that will need to be followed in order to ensure proper compliance. But as HHS intends to issue detailed compliance procedures, this could be a long time coming. With 2003 getting closer, organizations are urged to initiate implementation of their compliance policies without further delay. ◀

References

"Applicability of the Health Insurance Portability and Accountability Act of 1996 to Secondary Coverage and Continuing Coverage" [electronic version] (June 1999), *Insurance Standards Bulletin Series,* Health Care Financing Administration, pp. 99-01.

Excerpt from the Health Insurance Portability and Accountability Act (HIPAA) Concerning Self-Funded Non-Federal Governmental Plans (2001), *HIPAA Insurance Reform,* Health Care Financing Administration, p. 2721.

"HHS Issues First Guidance on New Patient Privacy Protections" [electronic version] (July 6, 2001), U.S. Department of Health and Human Services, pp. 1-2.

Kirschner, Richard. 2001. "An Analysis and Evaluation of the Principal and Recently Enacted Privacy Provisions of the HHS Regulations Promulgated Pursuant to HIPAA" [electronic version], *International Foundation of Employee Benefit Plans: HIPAA Privacy Rules Update,* I-VII.

Kongstvedt, Peter R. 1996. *The Managed Health Care Handbook* (3rd ed.). Gaithersburg, Md.: Aspen Publishing Company.

Kornetsky, Susan, and Judy Bauserman. 2001. "Employer Actions Required by the HIPAA Privacy Rules" [electronic version], *GRIST InDepth* 20010126. New York: William M. Mercer, Incorporated, pp. 1-6.

"National Standards to Protect the Privacy of Personal Health Information," *Federal Register,* December 28, 2000, pp. 160-164.

"Protecting the Privacy of Patients' Health Information" [electronic version] (April 23, 2001), U.S. Department of Health and Human Services, pp. 1-4.

"Questions and Answers on the HIPAA Nondiscrimination Requirements," U.S. Department of Labor, 2001, pp. 3-7.

"Standards for Privacy of Individually Identifiable Health Information" [electronic version] (April 6, 2001), *HIPAAdvisory,* pp. 1-30.

"State 'Succeeding Carrier' or 'Extension of Benefits' Laws and an Issuer's Obligation under HIPAA to Enroll an Eligible Individual Who is Disabled" [electronic version] (August 2000), *Insurance Standards Bulletin Series,* Health Care Financing Administration, pp. 00-04.