HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

by Laura Gerdes Bub

"Until now, virtually no federal rules existed to protect the privacy of health information and guarantee access to such information. This final rule establishes, for the first time, a 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 in their care." **Preamble to December 2002 Privacy Rule.**

This article discusses the HIPAA Privacy Rule focusing on the aspects of the Privacy Rule that are pertinent to municipal corporations.

Who Are "Covered Entities?"

The first and foremost question that arises when discussing HIPAA is: Does it apply to us? There are only three types of covered entities that must comply with the HIPAA Privacy Rule: (1) *Health Care Providers* are those persons or organizations that transmit any health information electronically in connection with a transaction covered by HIPAA and that provide medical or health services or that furnish, bill or are paid for health care services. (2) *Health Plans* are broadly defined and include most employer-sponsored group and self-funded health plans that provide or pay for medical care. Health plans also have been defined to include cafeteria plans or flexible benefit plans with medical savings accounts and employee assistance programs (EAPs). (3) *Health Care Clearinghouses* are public or private businesses or agencies that take health information from nonstandard format or content and convert such information into standard format or content, or vice versa. This article will touch on the Privacy Rule requirements for health care providers and health plans.

Oftentimes, only a portion of a particular entity satisfies the definition of a covered entity. In that circumstance, the entity may be a *Hybrid Entity.* A "hybrid entity" is a single covered entity that performs functions that are covered by the Privacy Rule and functions that are not covered. For example, cities having an Emergency Medical Services (EMS) Department may be considered a hybrid entity. In those situations, the hybrid entity must designate the operations of the entity that perform covered health care functions and those that do not perform covered health care functions. The hybrid entity also must establish firewalls so health information is not disclosed by the health care portion of the entity to the non-health care portion of the entity.

Before addressing the privacy regulations, it is crucial to know if a person or entity is a covered entity. The Center for Medicare and Medicaid (CMS) Web site has a "covered entity decision tool" which enables individuals and entities to determine whether they are a covered entity pursuant to HIPAA. This is a useful tool to determine HIPAA coverage. See www.cms.hhs.gov/hipaa2/support/tools/decisionsupport/.

What Are "Covered Transactions?"

The definitions to the Privacy Rule list the following transmissions of information between parties that are used to carry out financial and administrative activities related to health care: health care insurance claims; health care pay-

ments; coordination of benefits; health care claim status; enrollment/disenrollment in a health plan; eligibility for a health plan; health plan premium payments; referral certification and authorization; first report of injury; health claims attachments; and other transactions that the secretary of health and human services may prescribe by regulation. Accordingly, almost any transmission of information related to health care between two persons or entities constitutes a covered transaction. If one or both of the parties transmitting the information are covered entities, the Privacy Rule imposes strict regulations.

What Information Is Covered By HIPAA?

Protected Health Information (PHI) is individual identifiable information that is transmitted or maintained in any form or medium by a covered entity or its business associate and is maintained or transmitted orally, in writing, photographically, electronically, etc. *Individual Identifiable Health Information* (IIHI) is health information, including demographic information, that relates to an individual's past, present or future physical or mental health or to the provision of or payment for health care and identifies the individual (or the individual could reasonably be identified) and is created or received by a covered entity. Individual identifiers include a patient's or insured's name, address, birth date other than year, telephone/fax number, e-mail address, SSN, medical record number, plan I.D. number, account number, certificate/license number, VIN, vehicle serial/license number, URL address, URL or IP address, biometric identifiers (finger/voice/prints), photographic images, or other unique number, characteristic or code. Accordingly, any way in which a person may be identified is considered IIHI and if that information relates to health care and is maintained or transmitted by a covered entity, then it is PHI and is information that must be protected by covered entities under the HIPAA Privacy Rule.

What Is Not Covered Information?

Specifically exempted from a definition of PHI are education records covered by the Family Educational Rights and Privacy Act (FERPA) and employment records held by a covered entity in its role as employer. See 45 CFR §164.501. The final revisions to the Privacy Rule have clarified that covered entities that are employers (such as, cities, hospitals, health insurers) need not treat as PHI the health information that is held by the employer in its role as an employer. The focus must be on the reasons for which the entity has obtained or is using the health information. For example, health information that an EMS Department has collected pursuant to an employee's request for family leave is not subject to HIPAA's Privacy Rule, but health information maintained by the EMS Department when the employee utilizes its emergency medical services as a patient is protected under HIPAA. Other examples of health information that may be collected by an employer that is exempted from HIPAA includes information related to the ADA and similar laws, records relating to occupational injury, disability insurance eligibility, sick leave requests, drug screening results, fitness for duty tests and workplace surveillance. The Privacy Rule also is not meant to conflict with an employer's obligation to comply with laws such as workers' compensation and alcohol and drug free workplace laws.

The Privacy Rule

A covered entity may not use or disclose PHI except as required or permitted by the Privacy Rule. Disclosure only is required to an individual who is the subject of the PHI or to the Department of Health and Human Services (DHHS) to investigate compliance with the Privacy Rule. A covered entity is permitted to use and disclose PHI, without an individual's authorization, in three limited situations: (1) treatment; (2) payment; and (3) health care operations (TPO). "Treatment" means the provision of health care services by health care providers and includes consultants and referrals. "Payment" includes using and disclosing PHI to send invoices and file claims for billing purposes. "Health Care Operations" are numerous and include quality assurance activities, internal au-

dits, training, administrative functions and underwriting, rating and other activities necessary for the renewal or creation of contracts for insurance coverage.

Privacy Rule Requirements

As a covered entity, the Privacy Rule imposes many requirements. The following is a list of general requirements for covered entities. Some covered entities, such as certain types of health plans, will not have to comply with all or any of these requirements: (1) adopt a Notice of Privacy Practices (NPP); (2) furnish a NPP to all patients/members; (3) health care providers must obtain a signed acknowledgement of receipt of the NPP; (4) utilize patient authorizations; (5) impose minimum necessary standards; (6) consider routine incidental uses and disclosures; (7) execute "Business Associate" (BA) agreements with entities that perform services involving PHI; (8) identify all members of the workforce and their need to access PHI; (9) appoint a Privacy Officer; (10) ensure patient/member right to inspect, copy and request to amend PHI; (11) ensure patient/member right to request an accounting of PHI disclosures; (12) ensure patient/member right to request restrictions on uses and disclosures and alternative or confidential communications; (13) impose reasonable safeguards; (14) provide training to all members of the workforce; (15) adopt written policies and procedures, including employee sanctions; and (16) adopt a mechanism for resolving complaints regarding the handling of PHI.

"Minimum Necessary" Standard

Covered entities must use "reasonable efforts" to limit the use or disclosure of PHI to the "minimum amount necessary to accomplish the intended purpose." The minimum necessary rule does not apply to disclosures to the patient or individual, to DHHS, to disclosures to health care providers for treatment or to disclosures per a patient's authorization. To implement the standard, employers should categorize its workforce and identify what PHI is necessary for each category to access.

Permitted Uses And Disclosures Pursuant To An Authorization

A patient authorization is required for a covered entity's disclosure or use of PHI, unless the covered entity's use or disclosure is for TPO or some other permitted uses. Certain core elements must be included in all authorizations. The elements are set out in the Privacy Rule (45 CFR §164.508) and include, among others, a specific description of the PHI to be disclosed, the name of the "discloser" and recipient and the purpose of the use or disclosure.

Permitted Disclosures (45 CFR §164.512)

Certain uses and disclosures of PHI by a covered entity are considered "permitted disclosures" pursuant to the HIPAA Privacy Rule. Such disclosures include those that are required by law or that involve a public health activity, such as those compelled by the FDA or that concern transmission of a communicable disease. Other permitted disclosures (in-

volve abuse, neglect or domestic violence, judicial and administrative functions, limited disclosures to law enforcement and workers' compensation laws. Permitted disclosures also include those concerning decedents, organ transplants, research, prevention of a serious threat to health or safety, the military and veterans and correctional facilities.

Incidental Disclosures

A use or disclosure is allowed if it is "incidental" to an otherwise permitted use or disclosure and "reasonable safeguards" are in place. Examples of permissible incidents include semi-private rooms, waiting room sign-in sheets and calling out patients' names in waiting rooms.

Health Care Providers And Police Communications

A lot of discussion has gone on about the exchanges that occur on a day-to-day basis between covered entities which are health care providers, such as EMS personnel or hospital emergency room employees and law enforcement. As both entities have grown more accustomed to the requirements of HIPAA, some of these issues have been resolved. There are several permitted disclosures to law enforcement subject to the strict requirements of HIPAA and state law. Those disclosures include disclosures that are required by law, e.g., Missouri law requires reporting of certain wounds or injuries, disclosures pursuant to court order, court-ordered warrants or subpoenas and disclosures to law enforcement in response to specific requests using the "magic words:" "I am investigating a crime and need information to identify or locate a suspect, fugitive, material witness or missing person." Disclosures that are allowed to law enforcement also include those about victims of crimes, including decedents, and in an emergency care situation when necessary to alert law enforcement to a crime, location of a crime or victim or the identity and location of a perpetrator. See, 45 CFR §164.512(f).

Business Associate Agreements

Business Associates (BAs) are individuals or entities that perform a function or activity involving the use or disclosure of PHI (e.g., claims processors, billing companies, lawyers, vendors) on behalf of or for a covered entity. Covered entities must require BAs to sign a BA Agreement including "satisfactory assurances" that such entities will safeguard PHI.

Group Health Plans As Covered Entities

The second type of covered entity discussed in this article is "health plans." "*Group Health Plans*" are defined as health plans under HIPAA. A "group health plan" is an employee welfare benefit plan, including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement. The group health plan definition essentially covers all health plans, unless the plan is an employer plan with less than 50 participants and is administered by the employer.

Examples of group health plans include medical flexible spending accounts, dental plans, vision plans, major medical benefits and Medicare/Medicaid plans. Group health plans do not include disability insurance, auto medical payment coverage, liability insurance and workers' compensation insurance.

Privacy Rule Requirements For Group Health Plans

Many group health plans may be exempt from the full panoply of HIPAA compliance requirements listed above, depending on the administration of the health plan. Pertinent questions that health plan sponsors must ask are whether (1) the plan is fully insured or self-insured and (2) whether the plan creates or receives PHI other than summary health information or enrollment and/or disenrollment information. "Summary health information" is defined as de-identified information that summarizes claims history, claims expenses, or the types of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan. Such information is usually necessary for obtaining premium bids for modifying, amending or terminating the group health plan.

If a group health plan is fully insured and does not create or receive PHI, it is likely exempt from most Privacy Rule requirements. If, however, a group health plan is self-insured or fully insured and creates or receives PHI, then the group health plan is required to implement all of the HIPAA requirements pursuant to 45 CFR §164.530(k), including appointing a privacy officer, amending plan documents, implementing policies and procedures and the required notices, education and training and all safeguards.

Amending Health Plan Documents

A group health plan may only disclose PHI to its plan sponsor (HMO or health insurer), if the plan sponsor certifies that the plan documents have been amended to comply with the Privacy Rule. The employer/plan sponsor is essentially saying that it will only use and/or disclose PHI as allowed by law, for its "plan administration functions," "payment" and "health care operations." They also must ensure, among other requirements, that their agents and subcontractors abide by the same restrictions, report improper use and/or disclosure of PHI to the plan, allow indi-

viduals to inspect, copy, request amendments and accountings and not use and/or disclose PHI for any employment-related decisions.

Firewall Requirements

A plan sponsor must ensure that the plan documents are amended to provide for adequate separation between the group health plan and the plan sponsor. The plan sponsor must identify the employees/classes that will have access to PHI, restrict access to those employees for plan administration functions only and provide a mechanism for resolving issues of noncompliance. The plan sponsor also must adhere to all other administrative requirements similar to those of a health care provider.

Individual Rights

In general, individuals and patients have several rights under the HIPAA Privacy Rule. Patients are entitled to receipt of a notice of privacy practices and all patients/members are entitled to the right to inspect, copy and request amendment of their PHI, a right to an accounting, a right to request restrictions on uses and/or disclosures of PHI and a right to a confidential and alternative form of communication by the covered entity.

Compliance Deadlines

All health care providers and most health plans were required to implement the HIPAA Privacy Rule by April 14, 2003. A subset of the covered health plan, however, is the "small health plan." A small health plan is defined as a health plan with annual receipts of $5 million or less. (For clarification see, http://cms.hhs.gov/). Small health plans are required to comply with the HIPAA Privacy Rule by April 14, 2004.

Enforcement

The DHHS delegated civil enforcement of the HIPAA Privacy Rule to the Office of Civil Rights (OCR). Civil fines may be imposed for unauthorized disclosures of PHI in the amount of $100 to $25,000 per calendar year. Criminal penalties may be imposed for violations of disclosures of PHI from $50,000 to $250,000 and/or one to 10 years in prison, depending on the nature of the crime. However, no private cause of action exists under HIPAA.

Conclusion

This article is intended to review, in general, the aspects of the HIPAA Privacy Rule most applicable to cities, towns and villages. This article is not intended to be all-inclusive as the Privacy Rule includes many nuances that would be impractical to discuss here. Municipal corporations are encouraged to seek review by their own legal counsel relating to the specific concerns of each municipality and the HIPAA Privacy Rule.□

Questions may be e-mailed to the author, **Laura Gerdes Bub**, at lbub@cohgs.com or sent by mail to Laura Gerdes Bub, Curtis, Oetting, Heinz, Garret & O'Keefe, P.C., 130 S. Bemiston, Suite 200, Clayton, Missouri 63105.