By: Christine N. Bostick

HIPAA COMPLIANCE

Implications for ALM Members

The Health Insurance Portability and Accountability Act (HIPAA) is a complicated federal regulation that governs how healthcare providers, your clients, are able to use and to disclose confidential health information regarding patients. This is not a new subject for healthcare. Healthcare providers have always been sensitive to protecting inappropriate releases of confidential medical information. State and federal laws have also been around for many, many years addressing this same topic. HIPAA, in a very complex manner, attempts to tighten the reins on inappropriate uses and disclosures of this sensitive information, while at the same time attempts to achieve some uniformity throughout the country regarding health record confidentiality.

Development of HIPAA

Early efforts in dealing with the standardization of healthcare data, security, and privacy dates back to the 1960s, with studies first conducted by the National Committee on Vital Health Statistics. There were ever-growing congressional and public concerns related to breaches of healthcare privacy throughout the 1970s and 1980s. Americans became, and remain, increasingly concerned about personal exposure to vulnerability from wrongful disclosures of their health information. In fact, breaches of privacy make the most interesting headlines:

> *The medical records of a Maryland school board member were sent to school officials as part of the campaign criticizing his performance. The records revealed that the member had been treated for depression. (C. Samuels, "Allen Makes Diagnosis of Depression Public; Medical Records Mailed Anonymously," The Washington Post, August 26, 2000, p. V1)*
>
> *Thousands of medical records fell out of a vehicle and were blown throughout Mesa, Arizona. The records were being transported to be destroyed. ("Medical Records Fall Out of Vehicle, Blown Through Street," Associated Press, May 26, 2000)*

President Clinton's healthcare reform initiatives introduced in 1992 built on prior government recommendations to standardize electronic transactions in healthcare. In 1994, the press leak about tennis great Arthur Ashe's HIV status increased pressure to begin addressing privacy and security of health information, particularly if there are standards for electronic transactions increasing the use of this mode of transmitting information.

On August 21, 1996, HIPAA (also known as the Kennedy-Kassebaum Act, 42 USC 1320(d) et. seq.) was signed into law. HIPAA mandated that the Department of Health and Human Services (HHS) submit recommendations regarding privacy to Congress by September 1997, after which Congress would enact privacy legislation. Congress failed to agree on privacy legislation and missed its self-imposed deadline to pass a privacy bill. By law, the burden then fell on the Department of Health and Human Services to enact the necessary regulations to effectuate the law, and the first proposed privacy rule was issued on November 3, 1999.

After many reiterations and much public controversy over the privacy rules, final rules were published on December 29, 2000, and additional final revisions to the final rules were published on August 14, 2002. Healthcare providers had until April 14, 2003, to achieve compliance with a massive and complex set of health care privacy standards.

Key Principles of HIPAA

HIPAA applies to all healthcare providers, regardless of size, if they perform any of an enumerated list of transactions electronically. For most hospitals and health systems, HIPAA will apply and compliance is mandatory. HIPAA requires that healthcare providers implement certain specific steps in order to achieve compliance, including:

- Developing extensive policies and procedures to be adopted to ensure the protection of health information privacy.
- Recognition of new patient rights under federal law, including the right to access health information, the right to an accounting of certain disclosures of health information, the right to request corrections or amendments to their records, and the right to request restrictions on disclosures of patient health information.
- Appointing a privacy officer to lead the HIPAA privacy compliance program for the healthcare provider.
- Creating a lengthy written notice describing all the ways in which the healthcare provider may use or disclose a patient's health information, known as the provider's notice of privacy practices.
- Establishing a reporting and response system for privacy violations.

- Developing a policy for the discipline of HIPAA privacy violations by employees, agents, and contractors.
- Developing and implementing contract and amendment language for HIPAA compliance by healthcare vendors working on your behalf, also known as "business associates."

Business Associates under HIPAA

A healthcare provider is responsible for protecting an individual's privacy when using and disclosing protected health information. A healthcare provider will need to carefully track all of the ways in which protected health information is used and/or disclosed by both members of its workforce (including volunteers), as well as its business associates.

For a healthcare provider, a business associate is defined as a third party who has been retained by the healthcare provider to perform a service which involves the use or disclosure of a patient's health information. While an overly-broad generalization, the definition applies to third parties providing business advice or similar services to the healthcare provider, including accounting, billing processing, legal counsel, actuarial services, management services, and accreditation advice.

Common examples of business associates:

- Accountants
- Attorneys
- Billing Companies
- Billing/Coding Consultants
- Medical Record/Copying Services
- Transcription Service Providers
- Patient Translator Service
- Collection Service
- Document Destruction or Recycling Service

If the third party is a business associate, the healthcare provider must enter into a written agreement with the business associate which requires the business associate to recognize and operate consistently with HIPAA.

However, a business associate agreement is not needed unless the third party is truly a business associate, which means that you have been hired by the healthcare provider to actually use or disclose patient health information. The federal government has made clear in the August 2002 final rules that a business associate contract is not required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be de minimus, if at all. For example, a healthcare provider is not required to enter into a business associate contract with its janitorial service, because the performance of such service does not involve the use or disclosure of protected health information. In this case, where a janitor has contact with protected health information incidentally, such disclosure is permissible under HIPAA, provided reasonable safeguards are in place. Other common examples of business relationships that do not likely involve business associates:

- Maintenance and repair services (e.g., soda machine repair, electrical repair, or general office maintenance repair)
- Construction and renovation services (including electricians, plumbers, and handyman services)
- Delivery/courier services (e.g., delivery of medical or office supplies, FedEx or UPS deliveries, or water cooler refills)

Generally, commercial laundries with healthcare contracts will not be business associates of healthcare providers. Nevertheless, they may be asked to sign business associate agreements due to the fact that patient health information is often disclosed in the course of providing laundry services, etc. to the provider. They should not sign business associate agreements as a matter of course since they should not want to take on such legal obligations, but should perhaps consider executing a confidentiality agreement.

If the laundry is part of the hospital or healthcare organization, they are part of the healthcare provider, and they need to make sure they are working with nursing, and other members of the HIPAA compliance team, to make sure inappropriate disclosures do not occur. They need to make sure employees understand they must respect the privacy of protected health information, which is

more than just the medical or billing record. Any information that identifies, or could reasonably be used to identify, a person and their health condition (or payment for healthcare services) falls under HIPAA's regulatory scheme. This would include notes written on linens, empty IV bags left in the sheets, or physician/nursing progress notes that were not properly discarded.

Executing Business Associate Agreements

The HIPAA privacy regulations require that the covered entity (the healthcare provider) enter a written agreement with the business associate to receive assurances that the business associate will meet certain minimum standards in order to assure that the privacy of the individual's protected health information is maintained. The privacy regulations require that the business associate agreement:

1. Set forth the permitted uses and disclosures that the business associate is authorized to perform, which may already be detailed in an existing agreement between the parties.
2. Prohibit a business associate from using or disclosing health information, except as permitted by law or the agreement between the parties.
3. Require a business associate to have appropriate safeguards in place to prevent misuse or impermissible disclosures.
4. Report unauthorized uses or disclosures to the covered entity.
5. Seek assurances that if the business associate is permitted to subcontract, its subcontractors will also honor the HIPAA privacy requirements and the terms of the business associate agreement.
6. Make protected health information available to individuals for access and copying (Note: this should only be done within the parameters set by the covered entity or with the advice and consent of the covered entity.)
7. Make an accounting of disclosures as required by HIPAA available to the covered entity and the individual.
8. Make all practices, books, and records available to both the Provider and HHS, upon request, in order to assure compliance with HIPAA (Note: such disclosures, if related to the covered entity, should only be made after notice is provided to the covered entity.)
9. Agree to return or destroy protected health information on termination of the contract.

If the business associate fails to meet any of these standards, the covered entity must take action.

The options include:

- Always have an action plan to mitigate any violations.
- Terminate the contract with the business associate.
- If termination is not possible, contact HHS to discuss the situation and determine whether you may continue to do business with the business associate.

As you can see, the business associate contracts could be quite burdensome to implement and manage if you do not perform a service for the healthcare provider that directly involves the use or disclosure of patient health information. Releasing records, tracking the information obtained inadvertently, and making sure that information is properly destroyed or returned to the healthcare provider could be time consuming and costly.

What should commercial laundry managers do?

First, you will need to recognize that your clients are under a great deal of pressure to get complex regulations implemented in a relatively short period of time. Be patient with the healthcare providers and ask that they carefully explain to you why they believe you are a business associate.

Since the basis for identifying you as a business associate is likely because the healthcare provider recognizes that their employees are not diligent in making sure that private health information is not released to you–whether it is IV bags left in the linens, patient notes made on the bed sheets, or physician orders/progress sheets left in the laundry.

These disclosures are inappropriate and should be controlled within the healthcare provider. Making an ALM member a business associate does not solve the fundamental problem that these disclosures should be curtailed.

But you can offer some assistance to the healthcare provider. You can offer to educate your employees regarding confidentiality of patient information. Educate and train your employees about the fact that the healthcare clients are facing new and increasing pressures about the handling of confidential patient information. Seek assurances by way of a confidentiality statement from each employee that whatever information they may see or learn at work remains private. Also, discuss how you wish for confidential information to be handled. Is the healthcare provider comfortable with your disposal methods? If not, what compromise can be reached? Also, question if they would like any feedback on the amount of confidential information received. This may provide good advice and feedback to the healthcare provider working diligently to comply with this difficult law, allowing the healthcare provider to know what the employees are discarding through the laundry process and maybe, depending on your system, letting the healthcare provider know the amount of confidential information received relative to that received by peers/competitors. These options can be seen as marketing tools. Protecting confidences and secrets is good for business.

Please note: The following Privacy Standards information is provided for educational purposes and is not included in the tested material.

Privacy Standards

- Final Rules Published December 29, 2000
- Guidance Published July 6, 2001
- Final Rules Published August 14, 2002
- Compliance Date: April 14, 2003

All documents and information available at www.hhs.gov/ocr/hipaa.

Protected Health Information (PHI) regulated by HIPAA is information received, verbally or in written form, related to:

(i) the past, present, or future physical or mental health condition of an individual;

(ii) the provision of healthcare services to an individual; or

(iii) past, present, or future payment for the provision of healthcare to an individual. It either identifies the individual directly or it gives sufficient information that it is reasonable to believe that one could identify the individual based on the information available.

PHI is everywhere! To identify PHI, remember the following:

1. **PHI can be written or oral.** Healthcare providers often consider the actual medical record to be the extent of PHI. HIPAA extends this definition to billing information, as well as verbal communication. HIPAA does not require that every verbal conversation be documented, but it is important to consider that even a hallway conversation about an individual's bill or a medical condition is regulated as PHI.
2. **Information that relates to the past, present, or future physical or mental health condition of a patient is PHI.** Information about follow up appointments can be PHI.
3. **PHI is individually identifiable information.** Information that is unique to an individual that identifies the individual or could reasonably be used to identify the individual, linked with health information, is PHI. Even if information doesn't directly note the patient's name or health condition, if the sum of information "adds up" to reveal the individual's identity and health information, a privacy violation has occurred.
4. **PHI can be recorded on a variety of media.** IV bags, physician orders, notes on linens, faxes, medical records, x-rays, financial records, computerized data (e.g., diskettes or CDs), and physician dictation tapes are all PHI.

If a healthcare provider improperly uses or discloses PHI, or otherwise violates the privacy rules, serious penalties can be imposed. Possible penalties include:

- Financial: Fines of $100 per accidental violation, up to $25,000 per violation per year. Fines of up to $250,000 for intentional wrongful disclosures, such as disclosures for personal gain or commercial advantage.
- Prison terms: Sentences of up to 10 years for selling PHI for personal gain or commercial advantage.

In addition, the healthcare provider must have its own policies on HIPAA privacy violations, which include disciplinary action as severe as termination of an employee for misconduct.

1 LL

HIPAA Compliance: Implications for ALM Members

Earn one *Laundry/Linen* credit hour by completing the quiz over the material from this educational offering. To maintain ALM credentials, individuals must submit proof of continuing education in laundry & linen specific programs every three years. Access to contact hour quizzes are a benefit of membership in ALM.