Overview
A major problem with HIPAA is identifying information that is current and factually accurate, especially in view of the most recent amendments to HIPAA by the Omnibus Rule. The HIPAA marketplace is filled with volumes of valid, helpful information and tools. Most of it, however, is oriented to the hospital provider. The marketplace also contains much information that is outdated (written prior to the Omnibus Rule) and/or untrue. Without access to solid HIPAA expertise, an organization could easily spend considerable sums of money for bad advice and potentially noncompliance with HIPAA.

This article addresses special issues and concerns surrounding the implementation of a particular HIPAA regulation or its implementation in a particular segment of the health care industry. Writing a law that fits all industry settings is certainly daunting. In addition, covered entities and business associates must design a compliance program that fits the job they are doing and the level of risk they are willing assume. Many aspects of HIPAA are designed to be customizable and many industry segments such as Long Term Care and Home Health have developed HIPAA compliance guidance that addresses the issues unique to their industry and setting. This article speaks to those special program aspects and implementations.

Healthcare Education Programs
According to HIPAA (specifically, 45 CFR 160.103), “workforce” means “employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such entity or business associate, whether or not they are paid by the covered entity or business associate.

In dissecting HIPAA regulations from the educator's perspective:

1. Trainees are part of the healthcare workforce.
2. Education programs are part of healthcare operations.
3. Most training program relationships do not require business associate agreements.

---

1 The Omnibus Rule was published in the Federal Register at 78 FR 5566 (January 25, 2013).
The Clergy and PHI
HIPAA places limits on disclosure of information that a covered health care provider may provide to the clergy 45 CFR §164.510(a)(1)(ii). The provider may use or disclose the following information for directory purposes to members of clergy, as set forth at 45 CFR §164.510(a)(1)(i):

1. Individual's name;
2. Location in the facility;
3. Health condition expressed in general terms; and
4. Religious affiliation.

The rules state that the individual must have the opportunity to agree or object to the inclusion of their information in the organization's directory. Please see 45 CFR §164.510(a)(2)-(a)(3). Only the first three elements are available to the general public when inquiring for an individual by name according to 45 CFR §164.510(a)(1)(ii)(B). Religious affiliation is only available to the clergy and only if the patient has provided this information.

The Office for Civil Rights (OCR) Guidance Document of December 3, 2002 provided the following answer to the question: "Are hospitals able to inform the clergy about parishioners in the hospital?":

“Yes, the HIPAA Privacy Rule allows this communication to occur, as long as the patient has been informed of this use and disclosure, and does not object. The Privacy Rule provides that a hospital or other covered health care provider may maintain in a directory the following information about that individual: the individual's name; location in the facility; health condition expressed in general terms; and religious affiliation.

The facility may disclose this directory information to members of the clergy. Thus, for example, a hospital may disclose the names of Methodist patients to a Methodist minister unless a patient has restricted such disclosure. Directory information, except for religious affiliation, may be disclosed only to other persons who ask for the individual by name. When, due to emergency circumstances or incapacity, the patient has not been provided an opportunity to agree or object to being included in the facility's directory, these disclosures may still occur, if such disclosure is consistent with any known prior expressed preference of the individual and the disclosure is in the individual's best interest as determined in the professional judgment of the provider. See 45 CFR §164.510(a)."

In addition, the HIPAA Omnibus Rule at 45 CFR §164.510(a)(1)(ii) provides that use and disclosure of the information as enumerated above is permitted.

Clergy Policy
A policy and procedure on how the covered health care provider will deal with clergy and their access to patients and patient information will eliminate problems which might otherwise occur. For example, a major hurdle is defining who falls under the title of "clergy." This definition may vary with the nature of the covered health care provider. Many religious organizations have a lay visitor force that in the past has had open access to patients. In long term care, these visitors provide a valuable service calling on residents who may be far removed from their religious institution.
Anecdotally, one hospital defined clergy as someone who must have a religious institution and has attended special training with the covered entity’s chaplain. The hospital specifically excluded lay clergy from access to the directory even though the lay clergy were directly affiliated with a religious institution. Other hospitals have verified clergy credentials though their respective chaplain’s office and published a verified list to their respective local community. To be placed on the verified list, clergy must complete a brief application that is verified through the respective chaplain’s office, and then clergy must attend required training. While training includes privacy issues, such training may include general orientation to the covered health care provider, as appropriate.

**Shadow Charts & Independent Databases**

AHIMA defines a shadow record as “a duplicate record kept for the convenience of a department or healthcare provider. For instance, many emergency departments keep copies of an ER record for a few days or weeks in case of a readmission of a patient.” The privacy issues created by this parallel record system are discussed in detail in HIPAA Reins in Shadow Charts, Independent Databases [http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_021100.hcsp](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_021100.hcsp).

**Privacy Risk in Outsourcing**

Outsourcing has become an accepted practice in healthcare to reduce costs. This practice brings with it certain risks that must be considered particularly in terms of privacy and other legal issues. While the article Assessing Privacy Risk in Outsourcing [http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022546.hcsp](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022546.hcsp) focuses on outsourcing of medical transcription, it provides tips on contracting that can be applied to any business associate who will be handling protected health information. There is a list of questions that the provider should answer before selecting the best vendor for the job. The author also provides a list of actions the provider should build into any business associate agreement with the vendor in order to minimize risks. It also touches on the problems of outsourcing overseas where contractors or subcontractors may not be subject to US laws.

**Mental Health Information**

Privacy of mental health information is a complex and controversial subject. Many in the mental health sector of the industry believe that all health information should be treated with the same high level of confidentiality; that singling out mental health information for a higher level than general medical issues helps add to the stigma and “shame” frequently attached to mental health problems. Others believe strongly in the need to protect this sensitive information through legislation. Until the general public becomes more enlightened in its attitude toward mental health, we will continue to have a plethora of laws that carve out industry sectors with extra protections.

In general, the regulations that apply to a provider apply to a mental health setting except where preempted by contrary or more stringent laws. Management of mental health information is addressed in several places in the [HIMSS Privacy and Security Toolkit](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022546.hcsp). There is also an article that discusses privacy and confidentiality related to [alcohol and drug abuse](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022546.hcsp).
Privacy & Public Health
Shortly before the HIPAA Privacy Rule went into effect, the Centers for Disease Control and Prevention (CDC) and the Department of Health and Human Services published a guidance document “to help public health agencies and others understand and interpret their responsibilities under the Privacy Rule.” The document “HIPAA Privacy Rule and Public Health: Guidance from the CDC and DHHS" escorts the reader through the rule from the public health perspective, providing salient discussion and examples. The document may be accessed at: <http://www.cdc.gov/mmwr/pdf/other/m2e411.pdf >. Also refer to the article Privacy and Public Health elsewhere in the Toolkit.