

HIPAA and Higher Education

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is now upon us. Technologists will undoubtedly have heard rumors of the need for increased security regarding personally identifiable medical information, but the act is not that simple. HIPAA came about for several very good reasons, including the desire to leverage technology to reduce the cost of health care. The federal government estimates that 24 percent of health care costs are due to administrative overhead. Although HIPAA will initially require increased spending, the government estimates that when completely implemented, HIPAA will reduce administrative expenditures to between 6 percent and 16.5 percent of total health care costs.

HIPAA had its genesis in discussions in the organization that promoted EDI (Electronic Data Interchange) within the health care industry: Workshop for Electronic Data Interchange (WEDI). WEDI was formed by the Blue Cross and Blue Shield Association (BCBSA) and the Health Insurance Association of America (HIAA). Their initial goal was to come together and develop standards. Unable to reach an agreement, they turned to the Health Care Financing Administration (HCFA) of Health and Human Services (HHS) for help. Eventually this process attracted the attention of Congress, which hoped to leverage technology to reduce costs. In 1996, the Kennedy-Kassebaum Act (HIPAA) passed. In this act, Congress required itself to pass additional legislation by certain dates in four administrative areas, referred to as the administrative simplification portion of the act: (1) Identifier Standards, (2) Transaction and

Code Set Standards, (3) Privacy Standards, and (4) Security Standards. If no additional legislation was passed, HHS was required to issue rules for each of these areas. Since the HIPAA was intended to enable patients to move freely about the country and take medical information and insurance coverage with them, these areas were chosen as the points where standards would have the greatest impact:

- *Identifier Standards* were needed for employers, health service providers, and payors. Rules covering identification of employers, providers, and payors were proposed in 1998. Once published by HHS, these standards require compliance within two years after a sixty-day comment period. There was a proposed standard for an identifier for individuals, but it was shelved due to its controversial nature.
- *Transaction and Code Set Standards* were proposed in 1998 and became law in 2000; compliance is required by October 16, 2002. This section applies to transactions and the EDI commerce exchanged between and among providers and employers. The code sets are identifiers of the medical procedures.
- *Privacy Standards* were proposed in 1999 and became law in 2000; compliance is required by April 14, 2003. The purpose of these standards is to protect the privacy of individually identifiable information contained in transmission between and among employers and providers.
- *Security Standards* were proposed in 1998 and encompass electronic signa-

ture standards for certain transactions, among other requirements. Security standards also include all common practices, such as physical security of computer systems.

HIPAA mandates substantial penalties for noncompliance. For violations of code sets or other security infractions, a maximum of \$100 per person per violation of a provision, and not more than \$25,000 per person per violation of an identical requirement or prohibition for a calendar year—such as downloading 2,500 patient names to an unauthorized recipient—could be incurred.

HIPAA established more serious penalties for any person who knowingly or intentionally misuses a unique health identifier or who obtains or discloses individually identifiable health information. The penalties include (1) a fine of not more than \$50,000 and/or imprisonment of not more than one year; (2) if the offense is “under false pretenses,” a fine of not more than \$100,000 and/or imprisonment of not more than five years; (3) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than \$250,000 and/or imprisonment of not more than ten years. These penalties do not affect other penalties that may be imposed by other federal programs. Civil liability is specifically left in place as a potential remedy. Enforcement will be through the Office of Civil Rights on a complaint basis.

HIPAA requirements will touch every institution of higher education. The regulations specifically state that colleges

and universities are subject to HIPAA requirements. The impact will differ among institutions depending on how much personally identifiable patient information exists. An institution should create a task group or appoint a person to review HIPAA requirements and determine their applicability to the campus. This group or person will need training on HIPAA requirements. The next step will be to conduct a campus-wide assessment of the extent to which HIPAA rules apply. In the distributed environment of a typical campus, this requires careful analysis to discover the areas where

Higher education has considerable experience with the privacy of personally identifiable information, having dealt with the Family Educational Rights and Privacy Act (FERPA) of 1974 for twenty-seven years. The Privacy Rule of HIPAA is similar to FERPA, although an argument can be made that FERPA is more stringent because of its requirement for a signed authorization to be obtained before the release of personally identifiable information outside the institution.

Where must HIPAA be observed in higher education? The answer is anywhere that personally identifiable patient information is stored or transmitted.

Hospitals or clinics are clear examples. A not-so-obvious place might be the personnel office if employees are able to file health insurance claims through that office. If the institution is self-insured and uses a third-party administrator, then the enrollment and disenrollment information is protected. The Student Health Center does not fall under HIPAA because HHS has determined that student medical records are covered under FERPA—and

HIPAA must stop where FERPA begins. Those familiar with FERPA may remember that it exempts student medical records maintained by a physician or nurse. HHS has correctly determined that as soon as that record is seen by anyone else, including the student/patient, or as soon as it is used for any other purpose, it is an education record under FERPA and must be treated as such.

Interestingly, both HIPAA and FERPA address the concept of directory information but use opposite approaches. FERPA provides for opt-out, and HIPAA requires opt-in. In other words, under FERPA, students are included in the campus directories available to the public but must have the option to not have the information

published, whereas with HIPAA, personal information is included for public disclosure only after consent is granted with a written authorization.

Institutions with research efforts involving personally identifiable patient information will need to consider HIPAA requirements. One approach is to incorporate HIPAA requirements as part of the Institutional Review Board (IRB) consideration of human-subject research proposals. Patient consent forms will need to be reviewed for content, handling, and disposition in light of HIPAA.

Those familiar with the Federal Sentencing Guidelines, which would be used on conviction of HIPAA violations, recommend that each institution begin an in-depth training program for all staff members who deal with personally identifiable patient information. The goal of such a training program would be to make the protection of personally identifiable information a basic component of every employee's job.

The federal legislature has made several unsuccessful efforts to stop, delay, or change the regulations as currently proposed. Tommy Thompson, the new secretary of HHS, has clearly indicated that the Bush administration plans to implement the regulations with minimal or no changes and has already done so in the area of privacy. Final rules for the Security and Identifiers sections are expected before the end of the year, as are also comprehensive guidelines on penalties.

References

- Association of American Medical Colleges (AAMC). "Guidelines for Academic Medical Centers for Security and Privacy: Practical Strategies for Addressing the Health Insurance Portability and Accountability Act." <<http://www.aamc.org/members/gir/gasp/>> (accessed July 18, 2001).
- Family Educational Rights and Privacy Act (FERPA). 20 U.S.C. §1232g (1974).
- National Cancer Institute. "Confidentiality, Data Security, and Cancer Research: Report of a Workshop." <<http://www.nci.nih.gov/scienceresources/announcement/confintro.html>> (accessed July 18, 2001).
- U.S. Department of Health and Human Services. Administrative Simplification Web site: <<http://aspe.hhs.gov/admsimp/>> (accessed July 18, 2001).

C. W. Goldsmith is Vice President for Information Technology at the University of Alabama at Birmingham.



HIPAA must be observed. The objective at this stage is to create an understanding of what is required by the law, what the current practice is, and what must be done to close the disparity and achieve compliance. This entire process is commonly referred to as a "gap analysis." For example, in the fall of 2000, the University of Alabama at Birmingham appointed a HIPAA Compliance Steering Committee, which subsequently appointed subcommittees for each of the four administrative areas: Identifiers, Transactions and Code Sets, Privacy, and Security. These groups are identifying and refining assessment tools to be used across campus for self-assessment of compliance.