

**EDUCAUSE** Center for Applied Research

**Research Bulletin**

**Volume 2003, Issue 7**

**April 1, 2003**

# **Life with HIPAA**

## **A Primer for Higher Education**

Toby D. Sitko, EDUCAUSE Center for Applied Research

Norma K. S. Kenigsberg, New York University

Marilyn A. McMillan, New York University

Pietrina Scaraglino, New York University



## Overview

Colleges and universities that know they are subject to the privacy regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)<sup>1</sup> are, no doubt, well focused on the April 14, 2003, deadline for reaching compliance. Fueled by a combination of legitimate concerns and dramatic hype, the countdown to compliance is reminiscent of preparations for Y2K. Institutions racing to comply are advised to keep the momentum high. Unless government action is taken to change the requirements, compliance with the HIPAA regulations is likely to become an important obligation for many higher education institutions. Life with HIPAA has begun.

Because HIPAA includes complex legislation that impacts higher education but was not specifically written with academic institutions in mind,<sup>2</sup> some institutions still are unclear about whether they are subject to HIPAA. The purposes of this primer are to help identify the questions that higher education leaders can ask in determining if their institutions are covered by HIPAA and to provide some guidance on where to find answers. For purposes of this Research Bulletin, “HIPAA” refers to the HIPAA statute and its related regulations.

*Special Note: This document is not intended to provide legal guidance on the subject of HIPAA. Higher education officers are strongly advised to consult legal counsel to determine the degree to which their institutions are subject to HIPAA and their obligations for compliance.*

## Highlights of HIPAA

To understand HIPAA, it is useful to know the objectives of the law, some background about why it came into being, the three major sets of regulations that HIPAA comprises, the deadlines for complying with the regulations, the sanctions for noncompliance, and the agencies responsible for enforcement.

### Objectives and Background

The objectives of the HIPAA statute and regulations are to

- improve the portability and continuity of health insurance by providing mechanisms for maintaining health insurance when people change jobs;
- prevent and combat fraud and abuse in health care payment practices;
- promote tax-related health provisions, such as the use of medical savings accounts;
- change and standardize the way health care organizations exchange electronic health care data; and
- protect confidential, individually identifiable health care information and records through improved security standards and federal privacy legislation.

When the HIPAA statute was passed in 1996, its primary focus was on health insurance portability. Since most people in the United States have health insurance coverage through their employers, Congress wanted to relieve pressure on people who felt locked into their jobs for fear of losing employer-based health insurance covering health conditions that would be excluded from coverage by a new health insurer. The HIPAA statute also was intended to prevent health care fraud and abuse by adopting standards and requirements for electronic transmission of certain health information. It is interesting that in the early days of the statute, little attention was focused on the provision called “Recommendations with Respect to Privacy of Certain Health Information.”<sup>3</sup> All of this changed in December 2000.

### **Regulations and Compliance Deadlines**

On December 28, 2000, in response to authorization provided in the original HIPAA statute, the Department of Health and Human Services (HHS) issued the privacy regulations. Those regulations are one of the three sets of HIPAA-related regulations that have been issued. Table 1 identifies the three domains of HIPAA, including helpful nicknames for related regulations, full names and citations, and compliance deadlines. The nicknames for these regulations will be used throughout this Research Bulletin.

**Table 1. HIPAA Regulations and Compliance Deadlines**

<b>Regulation Nickname</b>	<b>What the Regulations Cover</b>	<b>Full Name and Citation</b>	<b>Compliance Deadline</b>
Privacy Regulations	Privacy of patient-identifiable information	Standards for Privacy of Individually Identifiable Health Information  45 C.F.R. § 160, 164 (2002)	April 14, 2003
ETS Regulations	Standardization of electronic transactions and code sets	Health Insurance Reform: Modifications to Electronic Data Transaction Standards and Code Sets  68 Fed. Reg. 8,383 (Feb. 20, 2003)	October 16, 2002, unless the ASCA one-year extension <sup>4</sup> request was filed by October 15, 2002. If the request was filed, the deadline to begin testing ETS compliance is April 14, 2003. The deadline for full compliance is October 16, 2003.
Security Regulations	Standards for the security of electronic, protected health information, to be implemented by health plans, health care clearinghouses, and certain health care providers	Health Insurance Reform: Security Standards  68 Fed. Reg. 8,334 (Feb. 20, 2003)	April 21, 2005

## Sanctions and Enforcement

Failure to comply with HIPAA carries significant sanctions. Risks associated with noncompliance include possible litigation, exclusion from participation in Medicare (for example, withholding of federal Medicare and Medicaid funds), and civil monetary fines of \$100 per infraction and up to \$25,000 per year for each violation. Sanctions for intentional violations carry criminal penalties, including fines and imprisonment.

On October 15, 2002, HHS Secretary Tommy G. Thompson announced<sup>5</sup> that the Centers for Medicare & Medicaid Services (CMS) will be responsible for enforcing the transaction and code set standards that are part of the administrative simplification provisions of HIPAA. On February 20, 2003, he announced that the CMS will enforce the security standards as well. The HHS Office for Civil Rights enforces the privacy standards.

## What HIPAA Means for Higher Education

There is broad agreement that HIPAA objectives are basically sound. Especially with respect to the HIPAA information security regulations, the standards reflect what is generally believed to be effective information technology practice for data and network security, administrative policy and procedure development, documentation maintenance and publication, and human resources training. While major universities with medical or dental schools or affiliated hospitals are concerned about the human and financial resources that must be allocated to achieve compliance with HIPAA because they deliver health care services in numerous ways, the impact on institutions will vary. Some states already regulate records management for health care delivery services to an extent that, in many respects, is equal to or more rigorous than HIPAA.

### Which Higher Education Institutions Are Affected?

“Covered entity” is the HIPAA designation for an organization or operation that is obligated to comply with HIPAA. These entities include health plans, health care clearinghouses, and health care providers—including some colleges and universities—that transmit protected health information (PHI) in connection with one of the electronic transactions covered by HIPAA described in Table 2. (See Table 4 for a description of PHI.) As a general guideline, a higher education institution is considered to be a HIPAA covered entity if it meets *both* of the following conditions:

- The institution provides health care services, *and*
- The institution engages in one or more of the “covered” electronic transactions listed in Table 2.

### Higher Education as a Health Care Provider

Although the primary mission of colleges and universities is educational, many institutions also provide health care in hospitals, clinics, and student health centers, or through affiliated faculty practices that provide patient care. Simply providing health care

services does not mean that an institution is defined by HIPAA as a covered entity. The institution must provide health care services *and* perform at least one of the covered electronic transactions listed in Table 2. For example, if an institution provides student health services and provides health care as part of a clinic, but neither of those functions engages in electronic transactions, then the institution might not be subject to HIPAA. The first and most important task for colleges and universities is to examine their internal operations carefully to ascertain whether any of their operations is subject to HIPAA. If any operation of the institution is covered, the institution must decide how it wants to declare its HIPAA obligation. Further discussion on declaring an entity type can be found below, under “Complying with HIPAA: The First Giant Steps.”

### Covered Electronic Transactions

Many health care and insurance transactions that take place within the institution, and between the institution and outside provider organizations, are transmitted via paper forms. Increasingly, however, these transactions are conducted either wholly or in part via electronic transmittal. Table 2 describes the 10 electronic transactions that would subject an institution to HIPAA.

**Table 2. Ten Electronic Transactions Covered by HIPAA**

HIPAA Covered Electronic Transactions
Health care claims or equivalent encounter information
Health care payment and remittance advice
Coordination of benefits
Health care claim status
Enrollment and 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

### Complying with HIPAA: The First Giant Steps

It is difficult to approach HIPAA in a small way. Even the first step, assessing whether a college or university is covered by HIPAA, is a big one. Following are some of the “giant” steps that an institution must take if it determines that at least some portion of it is obligated to follow the regulations. While these steps are presented sequentially, steps 2 and 3 can be undertaken simultaneously.

### **Step 1 (for all institutions): Determine Whether the Institution Is Covered**

The first job of any college or university with respect to HIPAA is to determine if any of the institution's operations is covered by HIPAA. If the institution does not provide *any* health care services, and if it does not conduct any of the transactions in Table 2 electronically, the institution likely is not covered. (It might, though, have HIPAA obligations as the sponsor of a health plan. For more on this, see the section below called "Group Health Plan Sponsorship.") Despite appearances, making this determination can be a difficult task.

Determinations about an institution's responsibilities under HIPAA can be made with internal resources, especially if counsel is familiar with the statute and regulations. Because HIPAA is relatively new and is not easy to interpret, colleges and universities also might want to engage outside counsel or consultants to help in the process. It is wise to specify that the outside resources must work collaboratively with the institution's legal counsel and operational leaders, both to help educate them and to be sure that the services are tailored to the particular health environment of the institution. Many consultants, including law firms and companies specializing in HIPAA assessment and remediation, offer services ranging from assistance in analyzing whether and to what extent an entity is covered by HIPAA to assistance in drafting policies and procedures and in training employees. Some firms specialize in privacy regulation services. Others can help assure that the institution's vendors are compliant with ETS regulations. Still others specialize in information security risk assessments, which typically involve network penetration testing, application and access vulnerability testing, and careful examination of internal policies, procedures, and personnel training practices.

Those institutions that determine they are a covered entity under HIPAA then can proceed to steps 2 and 3.

### **Step 2 (for covered entities): Establish a Governance Structure**

Institutions are advised to designate high-level administrators, such as senior vice presidents, chief legal counsel, and/or chief information officers, to oversee HIPAA compliance efforts. These individuals can appoint program management teams and appropriate committees and subcommittees to address the multitude of compliance assessments, analyses, and implementation activities. From the start, document the activities and decisions of these groups, and appoint an institutional liaison with each external consulting group that is engaged. It also is helpful to have a document repository accessible to the members of the working committees to house project plans, reports, meeting agenda and minutes, policies and procedures, and so on.

The HIPAA privacy regulations obligate covered entities to designate a chief privacy officer. The information security regulations, once they go into effect, require covered entities to designate a security official "responsible for the development and implementation of the policies and procedures required [under HIPAA]."<sup>6</sup> It is advisable for this latter official, whom some might call the chief information security officer, to hold these responsibilities institution-wide rather than just within the central information technology department. It is conceivable that these new roles can be performed by

individuals who already fulfill similar responsibilities at the institution. In other cases, institutions have established new HIPAA-specific positions. In either situation, it can be helpful to appoint these individuals early, if possible, so that they can lead or facilitate compliance efforts.

Although it might appear that responsibilities for compliance can be delegated to different officers of a covered institution, the regulations are so interrelated that they all must be understood by executive leaders. For example, the information security regulations are clearly in the purview of the senior information technology officer, but that same officer also must be involved with compliance with electronic transaction standards regulations if any institutional transactions use the campus network. Although the privacy regulations have the greatest impact on the operational units that provide clinical services (hospitals, medical and dental schools, student health centers), the regulations also may carry major ramifications for others who come in contact with PHI, such as researchers, legal counsel, development offices, internal audit, insurance, bursar, controllers (especially accounts payable), press and public affairs offices, and, of course, all information technology services.

It is important to note that in working toward compliance, covered institutions must be cognizant of state laws as well as HIPAA. In some cases, state laws are more stringent than HIPAA and must be followed.

### **Step 3 (for covered entities): Fully Covered or Hybrid Declaration**

Once an institution determines that it is subject to HIPAA, it must determine if it will be a fully covered entity or will designate itself a “hybrid entity.” A hybrid entity is defined as a legal entity that is a covered entity (it is a HIPAA-covered health plan, health care provider, or clearinghouse) whose business activities include both covered and non-covered functions. Because universities and colleges that provide health care services do so in addition to their primary activity (education), they have the option of declaring themselves hybrid entities with respect to HIPAA. Making this declaration involves identifying those components of the university covered by the regulations.

Declaring an entity type should be undertaken with careful consideration of the advantages and disadvantages of each type. Table 3 outlines some of the characteristics of each.

**Table 3. Hybrid and Fully Covered Entities**

Activity	Hybrid Entity	Fully Covered Entity
Application of Privacy Regulation Requirements	If an institution runs a clinic or other health care function that does not engage in electronic transactions, that health care component would not be covered by the privacy regulations in a hybrid entity. As a result, the uncovered health care component would not be required to provide patients with a notice of privacy practices, obtain HIPAA-compliant authorizations for the release of PHI, provide patients with accountings of disclosures of PHI, or undertake the myriad other obligations imposed by the regulations.	If an institution declares itself covered in its entirety, then all health care providers, regardless of whether they engage in electronic transactions, must comply with all of the requirements of the privacy regulations. Accordingly, all providers would be required to provide patients with a notice of privacy practices, obtain HIPAA-compliant authorizations for the release of PHI, provide accountings of disclosures and undertake the myriad other obligations imposed by the regulations.
Sharing PHI	If an institution runs a clinic that does not engage in electronic transactions, that clinic would not be covered by the privacy regulations in a hybrid entity. However, if covered components of the institution need to share PHI with the clinic, they would be able to do so only with patient authorizations.	If an institution declares itself covered in its entirety, then all health care providers, regardless of whether they engage in electronic transactions, can share PHI with other parts of the institution. The providers can do so without obtaining patient authorizations, subject only to applicable provisions of the privacy regulations.
Employee HIPAA Training	While it might be desirable for an institution to provide HIPAA training to its entire workforce, hybrid institutions are obligated to provide it only to persons who work in covered components. General awareness training should be provided to all those workforce members, and role-based training should be provided to specific audiences. HIPAA requires documentation related to training, so it is advisable to keep careful records from the start.	If an institution is a fully covered entity, HIPAA training must be provided to all workforce members. Some institutions elect to provide basic “HIPAA 101” training online and more advanced training to smaller audiences, either face-to-face or online. General awareness training should be provided to the entire workforce, and role-based training to specific persons. HIPAA requires documentation related to training, so it is advisable to keep careful records from the start.
Exposure to Criminal and Civil Sanctions	To the extent that HIPAA applies to covered components of a hybrid institution, the potential for penalties as a result of violations will focus on the activities of those in the covered components.	To the extent that HIPAA applies to all of a fully covered institution, the potential for violations spans a wider group of people: those in the entire institution.
Separation (Firewalls) between Health Care Components and Other Components of the Institution	Hybrid entities must create adequate separation, in the form of firewalls, between covered health care components and non-covered components. Determining where these firewalls should be, and impeding the free flow of information between covered and non-covered components of the institution, can be major challenges.	Fully covered institutions need not be concerned about separation between health care components and other components of the institution. Of course, they must vigilantly observe all regulations relating to confidentiality and appropriate use and disclosure of PHI to protect individual privacy.
Support Services	Hybrid entities must identify functional areas (such as departments) of the institution that provide support services to covered components, especially those that involve sharing of patient-specific health information.	Departments that provide support services are automatically included in fully covered entities.

## Special Considerations for Higher Education

Some universities and colleges may face unique challenges with respect to compliance with HIPAA. As institutions progress through compliance efforts, some will be surprised to learn which of their activities may be affected by HIPAA.

### Group Health Plan Sponsorship

Apart from whether institutions provide health care services, many will be affected by HIPAA because they offer health plan benefits to employees. Health plans are themselves covered entities under HIPAA—irrespective of whether the institution is a covered entity. As defined by the privacy regulations, a health plan is “an individual or group plan that provides, or pays the cost of, medical care” and includes both insured and self-insured group health plans.<sup>7</sup>

Colleges and universities should inventory the health benefits they offer and determine which benefits are subject to HIPAA. For example, group health, vision, dental, prescription drug, and long-term care plans are subject to HIPAA because they fall within the definition of a “health plan.” Conversely, disability, liability, and workers’ compensation plans are specifically excluded from the definition of “health plan” and are therefore not covered. Still other plans, such as life insurance and retirement plans, are not health plans because they do not “provide or pay the cost of medical care.” Even finer levels of granularity apply in the examination of cafeteria plans (typically not covered because they do not provide or pay the cost of medical care) and flexible spending accounts (typically covered because they do provide or pay the cost of medical care).

### Student Health Centers

University and college student health centers typically provide health care services to students. In some cases, they also provide services to others, such as faculty, staff, or family members. If a student health center provides health services (such as immunizations or pharmacy services) to people who are not students, and if it conducts one of the 10 HIPAA-covered electronic transactions listed in Table 2, the center is likely a covered entity under HIPAA. This is because the health records of the non-student population, by definition, are protected by HIPAA. If the center serves only students, it might be exempt from the requirements of HIPAA because HIPAA does not apply to student records covered under the Family Educational Rights and Privacy Act (FERPA) or to some of the specific health records that are exempt from FERPA. Current wisdom on this issue leans toward the interpretation that with respect to student health records, FERPA trumps HIPAA. Institutions are advised, however, to engage professional counsel before making a determination on whether their student health centers are covered under HIPAA.

### Research

Researchers and research universities have particular concerns about the effect of the privacy regulations on research that involves access to protected health information. For

universities that are themselves covered by the regulations, the concerns are twofold: with respect to the release of PHI for research, and with respect to the ability of the institution’s researchers to access PHI from other covered entities. In short, researchers can gain access to PHI, and covered universities can release PHI,

- with an authorization signed by the research subject,
- with a waiver from an institutional review board or privacy board,
- for a researcher’s review preparatory to research,
- for a researcher’s review of decedent’s information,
- if the PHI is de-identified, or
- if the PHI is partially de-identified and an agreement is entered into with the researcher.

HIPAA issues for research are numerous and complex. It appears likely that discussion on research-related issues for higher education will be animated, and solutions will evolve for some time to come.

Table 4 identifies definitions of PHI and de-identified information.

**Table 4. Protected Health Information and De-Identified Information**

Protected Health Information	De-Identified Information	Notes
<p>PHI under HIPAA means <i>individually identifiable</i> health information. <i>Identifiable</i> refers to data that are explicitly linked to a particular individual (that is <i>identified</i> information) and includes health information with data items that reasonably could be expected to allow individual identification.</p> <p>HIPAA defines health information as “Any information, whether oral or recorded in any form or medium” that</p> <p>“[i]s created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse”; and</p> <p>“[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.”</p>	<p>De-identified information is that from which all potentially identifying information has been removed. The privacy regulations specify 18 identifiers that, at a minimum, must be removed. (HIPAA also has a provision for a limited data set, from which most but not all potentially identifying information has been removed.)</p>	<p>Note that the definition of PHI excludes individually identifiable health information in education records covered by FERPA. It also excludes employment records held by a covered entity in its role as employer.</p> <p>HIPAA security, identifier, and transaction and code set rules, in contrast to the privacy regulations, cover only electronic information.</p>

## Curriculum and Student Practice

Higher education institutions involved in training of health care professionals should incorporate HIPAA awareness into their basic curriculum. At institutions that have programs in medicine, nursing, dentistry, and therapy, faculty most likely already are engaged in these efforts. With the expectation that our understanding of HIPAA will continue to evolve, the topic is particularly well suited to technology-assisted learning. HIPAA awareness training can be delivered as standardized, computer-based modules that easily can be updated as the application of HIPAA regulations becomes more widely understood. Technology can be used to help leverage the institution's HIPAA investments by sharing materials across programs.

It is important to note that students who practice as interns in facilities that are outside of the college or university are the responsibility of the outside facility. Because of this, institutions should pay particular attention to the affiliation agreements they have with these facilities to be sure that the agreements are consistent with this reality.

## Fundraising

Although HIPAA regulations were not intended to hamper the fundraising activities of higher education or other nonprofit organizations, the regulations might impact the way in which some institutions approach fundraising. Institutions should examine carefully their prospect-identification practices to be sure they are in compliance with both the letter and the spirit of the HIPAA privacy regulations. Protected health information—other than limited demographic information and dates of service—should neither be, nor ever appear to be, a factor in fundraising appeals without a patient's written authorization.

## Key Questions to Ask

Universities and colleges can be affected by HIPAA in a variety of ways. If institutional leaders have not yet begun asking questions, here are some to start with.

- Under the HIPAA definition of “covered entity,” is this institution covered by HIPAA?
- How will HIPAA compliance efforts be governed at this institution, in both the short term and long term?
- Should this institution be declared a “covered entity” or a “hybrid entity”?
- What are the HIPAA-related special considerations for this institution?
- When vendors advertise products that are “HIPAA-compliant,” with what, specifically, are they complying?

## Where to Learn More

- For expansion on this Research Bulletin, with extensive footnoting and citations to authority, please see Pietrina Scaraglino's article "Complying with HIPAA: A Guide for the University and Its Counsel," which is anticipated for publication in the *Journal of College and University Law*, Vol. 29, No. 3, 2003.
- Public Law 104-191, August 21, 1996. Health Insurance Portability and Accountability Act of 1996, <<http://aspe.os.dhhs.gov/admnsimp/pl104191.htm>>.
- Guidelines for Academic Medical Centers on Security and Privacy. Practical Strategies for Addressing the Health Insurance Portability and Accountability Act (HIPAA), <<http://www.aamc.org/members/gir/gasp/>>.
- EDUCAUSE Current Issues Resource Page for HIPAA, <<http://www.educause.edu/issues/hipaa.html>>.
- Phoenix Health Systems HIPAA Advisory, <<http://www.hipaadvisory.com/>>.
- U.S. Department of Health and Human Services, Office for Civil Rights HIPAA site, <<http://www.hhs.gov/ocr/hipaa/>>.
- U.S. Department of Health and Human Services, Administrative Simplification from the Office of the Assistant Secretary for Planning and Evaluation, <<http://aspe.os.dhhs.gov/admnsimp/>>.
- Centers for Medicare & Medicaid Services, HIPAA site, <<http://cms.hhs.gov/hipaa/>>.
- Covered Entities Decision Tools from the Centers for Medicare & Medicaid Services, <<http://cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp>>.
- Dixie B. Baker, *HIPAA Overview & Update*, version 0.12; November 11, 2002. SAIC Health Solutions, Inc., <<http://www.saic.com/healthcare/hipaa/HIPAAOverview.pdf>>.
- Provider HIPAA Readiness Checklist. This checklist relates to preparation for meeting the electronic transaction and code set requirements, <<http://cms.hhs.gov/hipaa/hipaa2/ReadinessChkLst.pdf>>.

## Endnotes

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (codified at 42 U.S.C. § 1320d-2(note)); Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002).
2. For instance, the privacy regulations as they relate to health care providers were designed for traditional providers, such as hospitals, dentists, and physicians, for whom health care is the primary responsibility. They do not take into account how health care traditionally is provided in an academic

medical center, university, or college. Consequently, the regulations are somewhat unrealistic and are challenging to adapt to an academic environment.

3. H.R. REP. No. 104-496, at 68 (1996) reprinted in 1996 U.S.C.C.A.N. 1865, 1868.
4. On December 27, 2001, President Bush signed into law H.R. 3323, Public Law 107-105, also known as the Administrative Simplification Compliance Act (ASCA). The ASCA is the law that provides for the one-year extension of the date for complying with the HIPAA Electronic Transactions Standard (from October 16, 2002, to October 16, 2003) for any covered entity that submitted a compliance plan to the Department of Health and Human Services by October 15, 2002. The ASCA also includes a provision that requires all Medicare claims to be submitted electronically after October 16, 2003. An exception applies to "small providers," which the ASCA defines as a physician, practitioner, facility, or supplier "with fewer than 10 full-time equivalent employees."
5. News Release, October 15, 2002, "CMS Named to Enforce HIPAA Transaction and Code Set Standards; HHS Office for Civil Rights to Continue to Enforce Privacy Standards," <http://www.hhs.gov/news/press/2002pres/20021015a.html>.
6. 68 Fed. Reg. 8333 (Feb. 20, 2003).
7. Standards for Privacy of Individually Identifiable Health Information Regulation Text, as amended, 45 CFR Parts 160 and 164, Section 160.103.

## About the Authors

*Toby D. Sitko (tsitko@educause.edu) is a Research Fellow with the EDUCAUSE Center for Applied Research. At New York University, Norma K. S. Kenigsberg (norma.kenigsberg@nyu.edu) is Information Technology Services Project Leader; Marilyn A. McMillan (marilyn.mcmillan@nyu.edu) is Associate Provost and Chief Information Technology Officer; and Pietrina Scaraglino (pietrina.scaraglino@nyu.edu) is Associate General Counsel. Kenigsberg, McMillan, and Scaraglino are actively involved in the NYU HIPAA compliance efforts.*

## Acknowledgment

The authors wish to thank Marie Pollio, a law student at New York University School of Law, for her research assistance.

Copyright 2003 EDUCAUSE and Toby D. Sitko, Norma K. S. Kenigsberg, Marilyn A. McMillan, and Pietrina Scaraglino. All rights reserved. This ECAR Research Bulletin is proprietary and intended for use only by subscribers. Reproduction, or distribution of ECAR Research Bulletins to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior permission is granted by EDUCAUSE and the authors.