The Privacy Argument

By Chris Kyriakakis, CPA, CISA, CIA and Sabrina C. Serafin, MA, MBA, CISA

INTRODUCTION

When we think about privacy, there are two major factors that appear to be driving the debate – availability of information and a willingness to share private information. Recalling consumers' attitudes regarding privacy 30 years ago, it was not unusual for people to share personal information such as their name, date of birth and political beliefs on their clothing, tattooed arms, buttons or bumper stickers. Today, those methods of communication have been complemented by social networking sites such as FaceBook, MySpace and Classmates.com. People of all ages are sharing, often as a demonstration of their artistic prowess, both superficial and deeply personal information. At the same time, many people in the past 15 years have gone from a simple entry in their local phone book to having a complete composite profile available on the Web.

Along with this change in attitudes towards privacy, there is an exponential increase in the availability of personal information. This is mainly due to the advances in storage capability, the proliferation of e-commerce and indexing innovations that make data availability almost instantaneous. This evolution of technology and desire to share personal information raises new questions, such as "what are the privacy expectations of the consumers?" and "what are the responsibilities of businesses and administrators to protect (and react) to personal information?"

Privacy is a nascent concept for many businesses and industries; however, there are several industries where privacy risks have been catapulted to the foreground. Higher education is one of those industries. Soon after the Virginia Tech tragedy in April 2007, many eyes turned to the complicated privacy laws that impeded the sharing of information between education, law enforcement and healthcare. As often happens in the wake of a tragedy, rules and regulations were examined and revisions proposed to address a situation that until that time was incomprehensible.

As an auditor, it is necessary to understand the risks that create significant exposure to the organization and the expectations of administrators to mitigate those risks. In this article, we will provide a background of the evolving privacy requirements as risks to institutions of higher education and a framework for performing a privacy audit.

PRIVACY AND DATA PROTECTION

In general terms, privacy encompasses the rights of individuals and the obligations of organizations with respect to the collection, use, disclosure and retention of personally identifiable information. "Personally identifiable information" refers to any information that identifies or can be used to identify, contact or locate the person to whom such information pertains. This type of information, regularly utilized by academic institutions, is subject to certain data protections. While regulation is in place to guarantee students the right to privacy (see Family Educational Rights and Privacy Act or FERPA), student data is particularly vulnerable due to the vast need to share and distribute student data within the academic institution (e.g., among departments) and externally (e.g., transcripts).

KEY REGULATIONS

Managing privacy risks often starts with understanding the regulations and authoritative guidance governing the institution. Two significant privacy laws enacted to protect students are FERPA, as it relates to sharing of educational records, and the Health Insurance Portability and Accountability Act (HIPAA), as it relates to sharing of health and treatment records.

FERPA

FERPA, enacted in 1974, was designed to protect students' personal information from such mundane exposures as having their grades posted on a bulletin board to more intricate requirements on how the states may transmit grades to federal agencies. As it currently stands, FERPA provides basic protections for students and parents. The requirements relate only to colleges, universities, and other educational agencies that receive federal funding. FERPA's primary requirements for the schools include:

- Providing students over the age of 18 access to inspect their educational records
- Providing students with copies of their educational records upon request
- Redacting personally identifiable information about other students that may be included in a student's educational records

(see "The Privacy Argument," page 10)

ABOUT THE AUTHORS

Chris Kyriakakis, CPA, CISA, CIA *leads Frazier & Deeter's Information Technology Assurance and Governance Services Group where he specializes in implementing Enterprise Risk Management, IT Governance, and SAS70 Audits. He is a former PCAOB inspector and formerly from Deloitte & Touche LLP.*

Sabrina C. Serafin, CISA is a Senior Manager in Frazier & Deeter's Information Technology Assurance and Governance practice. She specializes with consumer privacy services. Sabrina was formerly a Director of Internal Audit at CheckFree Corporation where she implemented and supported their privacy program.

(continued from "The Privacy Argument," page 7)

- Consideration of a request to amend inaccurate or misleading information
- Providing a hearing if the request above is declined
- Requiring a student's consent (signed and dated) before disclosing educational records
- Annually notifying the students of their rights under FERPA.

As a note, these protections are largely granted to parents when the student is under the age of 18 and the protections relate to educational records and specifically exclude health records that might be held by the institution. *(Paraphrased from US Department of Education Web site)*

HIPAA

Originally enacted in 1996 to regulate the healthcare industry, HIPAA was created in response to the increasing ease of sharing health information electronically between doctors, medical organizations and insurance companies. A specific section of the Act, referred to as the Privacy Rule, focuses on the protection of private information. The Privacy Rule took effect in 2003 and spawned the recognition of a new term, Protected Health Information (PHI). PHI is any information regarding the health status, healthcare or payment of services that can be linked to an individual (e.g., names, SSNs, medical treatments, diagnoses, etc.). Some of the significant requirements of a healthcare institution include:

- Documented privacy policies and procedures
- A designated privacy official to develop and implement the policies and procedures
- Training and communication of the policies and procedures
- Proper administrative, technical and physical safeguards to protect PHI from being disclosed in violation of HIPAA
- Documentation and record retention requirements that extend six years for documents and records identified under the Privacy Rule. *(Paraphrased from the US Department of Health and Human Services Web site).*

FERPA and HIPAA are only two, albeit the largest, examples of an amalgamation of complicated state and federal laws designed to protect consumers' information. It is this complexity that has been deemed by many as one of the major obstacles in preventing the Virginia Tech tragedy.

As a result, new legislation was proposed in early 2008 to amend FERPA and to simplify some of these unnecessary complexities. The proposed amendments would give more latitude to educational administrators and allow them to share personally identifiable information without the consent of the student when certain circumstances arise. The updated language also clarifies FERPA rules of disclosure when required under the US Patriot Act and the Campus Sex Crimes Prevention Act.

Considering the complexity of privacy laws and the inability of many to keep their personal information secure, it is becoming a greater challenge for institutions to manage their risk policies and for auditors to evaluate and report on the design and implementation of those policies. For many audit departments, privacy has become one of the top compliance and reputational risks in their organizations.

PRIVACY IN ACADEMIC INSTITUTIONS

The news is inundated with stories of privacy breaches in every industry, and academic institutions are not immune to scrutiny. Regardless of a university's existing privacy policy and practices, auditors must gain an understanding of the effectiveness of the supporting processes. Enter the privacy audit.

MECHANICS OF A PRIVACY AUDIT

A privacy audit examines the policies and procedures surrounding the collection, use, disclosure and retention of personally identifiable (and often proprietary) information that is commonly utilized by academic institutions. Auditors must ensure that information processing controls are sufficient to meet privacy requirements and standards by reviewing the ways in which information is used, handled, modified and manipulated. Below are four steps for auditing privacy, along with questions to ask to determine the status of privacy protection within the organization.

Identify Privacy Risks

The most important step in a privacy audit is to identify the privacy risks that are present throughout the institution. The auditor must gain an understanding of how personal information is collected, used, stored and disclosed and then must evaluate the potential privacy risks to that information.

One of the most effective and thorough means to identifying these risks is to gain an understanding of how data flows through the organization. Each data access point can be considered a potential risk area. For each data access point:

- Understand what protection mechanisms are in place and who is responsible for implementing them
- Determine how personal information is used at that point and to whom it is disclosed
- Ascertain whether outside organizations are allowed access to the information and how that happens.

Evaluate Existing Policies and Procedures

Once the universe of privacy risks has been established, it is important to understand what policies and procedures are in place to govern privacy and manage those risks. Consider the information management procedures and the processes for collecting, maintaining and using

personal information. What is the process for managing privacy and confidentiality issues? Answers to these questions will help the audit team better evaluate and quantify the risks identified in the first step.

Test Key Controls
A basic understanding of risks and the corresponding controls will point to the tests necessary to truly reveal the organization's formal and informal privacy practices. Testing of key controls will include:

- Access controls that are in place to protect personal information from unauthorized modification or use, damage and loss
- Procedures for password use
- Procedures for database administration
- Personnel procedures
- Control procedures for the wide-area network and local area networks
- Physical security of the computer systems
- Procedures for the storage and disposal of data output.

Assist Management with the Resolution of Findings and Issues
Following testing, results must be summarized and reported in a way that guides the organization toward a comprehensive plan to mitigate privacy issues and findings. The report will be geared toward the organization's particular needs, helping it migrate to a strong privacy management program. Findings will provide recorded assurance that privacy issues have been appropriately identified, adequately addressed or brought to senior management for further direction.

Typical recommendations include:

- Limit access to those who require it
- Adequately secure data
- Publish the corporate privacy policy; train employees
- Manage data in accordance with sensitivity
- Build an incident response plan
- Limit sensitive data collection and posting
- Verify compliance with privacy regulations
- Establish information retention and destruction rules
- Require and enforce confidentiality and non-disclosure agreements.

Identified risks and solutions should be used by the organization to remediate gaps in business processes and procedures to better protect sensitive data, comply with laws governing data security, develop effective compliance strategies and put best practices into action.

SUMMARY

As custodians of private data, the responsibility of educational institutions should be to formulate, plan, implement and support privacy standards and tools protecting the personally identifiable information of faculty, staff, students and graduates. Structuring an academic privacy program requires the ability not only to deal with where data collection, access and disclosure may provide risk at a given point in time, but also the ability to change within a rapidly evolving environment. Auditors are in place not only to ensure that the collection, access and display of data are in compliance with expectations, privacy laws and standards, but also to provide a framework and guidance for that compliance. ■

(continued from "Values and Visions," page 3)

Another way to support camaraderie is to continue development of the ACUA ambassadors. This is a group comprised of longtime members with a history of involvement in ACUA activities. This group might include past Board and Committee Chairs, Board or Committee members, and individuals who are willing to extend the reach of the Board by attending the first-timers reception and watching out for individuals who appear disconnected at conferences. These individuals will continue to play other important roles in ACUA's future, such as representing our group with other associations.

Goal B: ACUA will be the principal advocate of internal auditing in higher education.

We also want to continue developing the "ACUA Risk Dictionary" by using it to communicate risk and controls on emerging areas important to higher education. We have spent a lot of time and effort on this project and I believe it is not only one of the most valuable member benefits, but is also vital to the achievement of our vision. When Kevin Robinson, Mark Paganelli and I met with representatives of the Association of Governing Boards (AGB) and the National Association of College and University Business Officers (NACUBO), they were both impressed and extremely interested in this project.

Goal B: ACUA will be the principal advocate of internal auditing in higher education.

Kevin Robinson began the process of formalizing agreements and relationships with other higher education groups like AGB, NACUBO and the University Risk Management and Insurance Association (URMIA). Fostering these relationships will benefit ACUA members. He will continue those efforts as immediate past president.

I believe ACUA has come a long way thanks to the innovative ideas, hard work, and dedication of ACUA members, both past and present. But much more can still be done to make ACUA a recognized leader in higher education. It does take a "Village," so please contact Mary Barnett (ACUA Volunteer Coordinator) or any of the Board members if you are interested in volunteering for any of our important activities. ■