Beyond FERPA: Maintaining the Privacy and Confidentiality of Student Data

Dr. Melisa N. Choroszy
Associate Vice President for Enrollment Services
University of Nevada, Reno

Colleges and universities have depended upon the Family Education Rights and Privacy Act, better known as FERPA, or the Buckley amendment, to guide them in the development of their principle policies and practices governing the release of student data. With the development of the electronic world, the demand for instantaneous access to information and the immediacy of transactions and integration of data, the need for additional controls to maintain privacy and security across all venues surfaced with the Gramm-Leach-Bliley Act of 1999 (GLBA). May 23, 2003 was the date that all institutions public and private, corporate or non-corporate, educational and non-educational were required to demonstrate compliance with this act.

The Gramm-Leach-Bliley Act of 1999 is also known as the Financial Services Modernization Act. It is intended to protect consumers and customers who obtain “financial products or services to be used primarily for personal or other household purposes”. Financial institutions are required to provide customers with notice of privacy policies and practices which describes how it may disclose nonpublic personal information about consumers to nonaffiliated third parties. Consumers must be provided with an opportunity to opt out. In addition, this opportunity must be made available to all customers at the beginning of the financial relationship and annually thereafter. Institutions of higher education are considered financial institutions as they do lend funds to consumers. However, institutions of higher education are exempt from the requirements of the privacy policy under GLBA, if those institutions are in compliance with FERPA.

While institutions of higher education are deemed to be compliant with the privacy requirements of GLBA, compliance with FERPA alone does not satisfy the requirements of the safeguarding regulations of GLBA. Institutions of higher education are required to adopt an information security program. Some of the key elements of the safeguarding provision which must be addressed include the designation of an employee who is responsible for the coordination of the information security program, the identification of risks to the security of customer information, and the requirement that all service providers implement and maintain safeguards. The design and implementation of safeguard programs need also include a policy on employee training whose purpose is to communicate responsible practices, common safety rules as well as each institution’s privacy policies.

A designated person or persons from each institution must be identified as those responsible for program coordination. Most institutions have designated their Chief Information Officer and at least one other person ranging from their internal auditors and chief business officers to their chief student affairs officers. These individuals coordinate the required elements of the program. They are also responsible for development and update of the institution’s security plan as well as the coordination of all compliance reviews and adjustments.

Risk assessment is an important element of GLBA and the Federal Trade Commission has identified four areas that must be addressed: (1) Information Systems, (2) Employee Management and Training, (3) Managing System Failures and (4) Service Providers. The identification of risk is necessarily as ongoing process as new technologies are implemented. A mechanism for the continued identification of these risks is coordinated by the designated program coordinator(s).
The identification of risks is interpreted as both internal and external and must be defined by each institution. Arizona State University has defined their Information System Risks as: (1) the unauthorized access of Protected Information by someone other than the owner of the covered data and information, (2) system security compromised as a result of system access by unauthorized persons, (3) the interception of data during transmission, (4) the loss of data integrity, (5) errors introduced into the system, (6) corruption of data or data systems, (7) the unauthorized access of covered data and information by employees, (8) unauthorized requests for covered data and information, (9) unauthorized access through hard copy files or reports and (10) unauthorized transfer of covered data and information through third parties. (http://www.asu.edu/privacy/security.html) Policies regarding the use of electronic resources must also be in place.

Employee Training must be addressed within the context of the safeguard provision. For those individuals who access student data, FERPA training needs to be provided. The University of North Carolina provides information about its FERPA training on the web at this address: http://regweb.unc.edu/official/training/FERPA.html. Employees at UNC receive a copy of the document “Maintaining the Security, Confidentiality, and Integrity of Customer Information”. Provisions need to be made for refresher training as part of the safeguard requirement. In addition, those who provide services to institutions of higher education must also agree to the provisions of GLBA, assuring both the privacy and safeguarding of customer information, including the unauthorized release of confidential data to third parties.

The provisions of GLBA may seem obvious to Registrars and Financial Aid Officers who vigilantly protect the confidentiality of student data. Compliance with GLBA provides us with the opportunity to remind our colleagues across campus of the critical importance of this vigil. While most institutions have always provided for the safety and security of campus data, GLBA makes very clear the need for the coordination of data use and the codification of data policies on campus. The premise of GLBA is simple. Be responsible in the use and release of confidential data, keep it secure and provide access only to those who need it to get their job done.

The Campus Legal Information Clearinghouse provides a generic template for the development of the security plan which can be found at the following web location: http://counsel.cua.edu/glb/resources/baylor1/ cf m

An inventory of best practices regarding the assurance of confidentiality and security is available at www.naaccr.org.

Other models of university sites for GLBA compliance include:
http://www.georgetown.edu/policy/glb a
www.vpfa.fsu.edu/policies/bmanual/safeguard.html
http://www.asu.edu/privacy/security.html