New Regulations: GLBA Safeguards Rule for Higher Education

ARTICLE 07.17.19 DEAN DORTON

The five year wait is finally over. In 2014 the Department of Education (ED) issued a Dear Colleague Letter notifying Colleges and Universities they would need to be compliant with data safeguard rules applicable to the Gramm-Leach-Bliley Act (GLBA). The 2019 OMB Compliance Supplement was released July 1, 2019 and it does include new GLBA Data Safeguard requirements.

What is GLBA & How Does it Affect Higher Education?

In order to operate successfully, colleges and universities must acquire and maintain an incredible amount of sensitive student personal and financial information. So it is vital — and incumbent upon those institutions — to keep this information safe and well protected at all times.

The Gramm-Leach-Bliley Act (GLBA) is in place to address a variety of consumer financial privacy concerns, including those related to the transfer and safety of personal and financial information of college students.

Enacted in 1999, GLBA is a regulation under the Federal Trade Commission (FTC) that requires financial institutions to be transparent about information sharing practices and to safeguard sensitive information. Also called the Financial Services Modernization Act of 1999, the purpose of the GLBA was to allow consumers to take advantage of the benefits of financial mergers while maintaining the integrity and security of banking and financial systems.

It's important to note that GLBA only applies to Colleges and Universities under Title IV due to the administration of student financial aid programs. Also, it is effective for Colleges and Universities with fiscal year ends ending June 30, 2019 or later.

While we have had plenty of time to plan for GLBA and pour over the guidance issued since 2014, the guidance was not very specific. We were not entirely sure what to expect. The 2019 Compliance Supplement does not contain all the GLBA Safeguards Rule elements, but only a subset. Will more come? Is the plan to phase additional requirements in each year? Will these be all we see? The answers are, "We do not know at this point," and no guidance has been provided yet on future plans. Either way, the good news is the first year requirements are less stringent than they could have been.

So what are the rules? They are summarized in the following three audit procedures:

1. Verify that the institution has designated an individual to coordinate the information security program.
2. Verify that the institution has performed a risk assessment that addresses the following three required areas.
    - Employee training and management;
    - Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
    - Detecting, preventing and responding to attacks, intrusions, or other systems failures

3. Verify that the institution has documented a safeguard for each risk identified.

How to Stay Compliant with the Safeguards Rule?

The Safeguards Rule makes it imperative for higher education institutions to create and maintain an information security plan that follows certain parameters to adequately protect customer information. GLBA Safeguards Rule requirements for colleges and universities include:

- Development of a written plan that describes their program to protect customer information, and must be suitable for the institution's size and complexity, and sufficient for the nature of the activities and sensitivity of the information involved.
- One or more employees to be designated to (and will be responsible for) coordinating the safety program.
- A method to identify and assess current risks to customer information in each relevant area of the informational system, and evaluate the effectiveness of the way these risks are currently controlled.
- Safeguards for potential risks must be set in place and routinely tested and monitored.
- Service providers must be qualified to maintain appropriate safeguards.
- Evaluations and adjustments when relevant situations arise, like changes in business operations or results of security testing.

These regulations are designed to provide the flexibility colleges and universities need to create security programs based on the institution's unique size, scope, and context. For any information security plan to work effectively, all employees should be aware of the policy and how it works, and it's recommended that frequent reminders be posted to help employees recall the requirements and understand the legal ramifications of failure to comply.

Risks of Non-Compliance

As cyberattacks continue to become more sophisticated, devious, and frequent, colleges and universities are becoming prime targets of hackers and ransomware. As they will continue to experience the consequences of major computer system breaches, the U.S. Department of Education (ED) has emphasized the importance of colleges and universities taking appropriate measures to protect sensitive data.

Failure to maintain compliance with FTC regulations can lead to serious consequences, including fines and public reports that make institutions in question far less attractive to incoming students. Perhaps most importantly, colleges and universities that suffer cybersecurity breaches are at risk of restricted or complete loss of Title IV funding, making them ineligible to participate in federally funded financial aid programs.

3 Tips for Higher Education Institutions to Maintain GLBA Compliance

To provide peace of mind for parents, students, and the institutions themselves, certain precautions can be taken to make it easier to follow GLBA standards. These include:

1. Take Special Precautions When Hiring New Employees

Check references and backgrounds for those who will be responsible for sensitive information, limit access to sensitive information, and require strong passwords that must be changed routinely.

2. Routinely Remind Employees of Important Information Safety Policies and Disciplinary Actions

Policies should be shared with employees and posted where they can be easily accessed, with reminders about specific disciplinary measures for all policies.

3. Maintain a Strong Working Relationship With Your Software Developers

Monitor the websites of your software vendors for recent information about emerging threats, check with vendors for patches that reveal vulnerabilities, and use antivirus and spyware programs that update automatically and maintain up-to-date firewalls.

Dean Dorton's IT Audit and Cybersecurity Assessment team specialize in providing IT risk assessments and audits to help keep colleges and universities compliant with the new GLBA Data Safeguard requirements. Is your institution too small to hire an information security officer? We understand the budget constraints on today's colleges and universities and can provide team members to be your institution's information security officer and consulting around hiring and coordinating your information security program.