BitLyft
Cybersecurity

GLBA GUIDE FOR HIGHER EDUCATION

COMPREHENSIVE GUIDE

A helpful step by step guide and checklist for meeting GLBA compliance requirements.

History

Timeline 2
A Short History 3
Education Department Ruling 4
Breakdown of Each Section 5
What's at stake? 8
Best Practices 9
Checklist 10
The BitLyft Approach 11

TIMELINE OF GLBA

1999

GLBA LAW PASSED

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, passes in 1999.

2001

GLBA COMPLIANCE REQUIRED

The GLBA act finally becomes required after a 2-year grace period for getting ready for compliance.

2002

SAFEGUARD RULE (16 CFR 314 INTRODUCED)

FTC introduces the Safe Guard rule for organizations under their jurisdiction to keep customer information secure.

2003

SAFEGUARD RULE REQUIRED

Rule becomes required after a short grace period for compliance.

2016

FSA DEAR COLLEAGUE LETTER (GEN-16-12)

Letter reminds institutions of their legal obligation to protect student information used in the administration of Title IV programs.

2018

FSA AUDITING FOR GLBA

Federal student aid starts auditing procedures to assess institution's capabilities in securing student information regarding Title IV programs.

2020

FSA CYBERSECURITY ENFORCEMENT GUIDANCE

FSA emphasizes heightened accountability to comply with GLBA requirements through annual compliance audits.

HISTORY

The Gramm-Leach-Bliley Act (GLBA) is also known as the Financial Services Modernization Act of 1999. The law was originally passed to allow different types of financial institutions to merge. These mergers created new challenges and risks with the sheer amount of customer information combined into one institution. The law included rules on how financial institutions (including the larger ones) would have to protect consumer financial information. These rules are known as the Privacy Rule, the Safeguards Rule, and the Pretexting Rule. They are enforced in various industries by respective regulating bodies like the federal bank regulatory agencies, the Securities and Exchange Commission, and the Federal Trace Commission (FTC).

Understanding GLBA and its rules and how they apply to higher education can be confusing and hard to navigate.

Meeting compliance and operating with best practices to maintain safety of sensitive information is a necessary hurdle institutions will have to master to ensure they still receive federal funding. Higher Education institutions are under GLBA because they participate in financial activities that are defined in banking law; like administering federal student loans. However, because colleges and universities don't entirely fit the traditional model of a financial institution, the FTC has provided some flexibility.

The Privacy Rule regulations created by the FTC state that colleges and universities are deemed to be in compliance with the rule if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). Thus, colleges and universities do not have to bear the unique burdens of the Privacy Rule in addition to those they must already address under FERPA.

EDUCATION DEPT RULING

On February 28, 2020, the Federal Student Aid (FSA) office of the U.S. Department of Education (DoE) released new guidance for colleges and universities on the security of student financial aid information. A Dear Colleague Letter GEN-16-12: Protecting Student Aid Information expands on a similar previous letter in which FSA highlighted institutional responsibilities under the Student Aid Information Gateway (SAIG) Enrollment Agreement as well as the Gramm-Leach Bliley Act (GLBA) and other laws to protect student financial aid information from unauthorized disclosure or access.

FEDERAL STUDENT AID RULING

FSA's 2020 letter emphasizes GLBA compliance by stating that it will soon begin holding institutions accountable for fulfilling GLBA Safeguards Rule requirements. And therein lies the importance of higher education institutions being prepared and able to meet compliance before an audit deems them in violation. A lack of compliance could risk losing necessary federal funding and create severe consequences to institutional reputation.

Financial audits of higher education institutions are triggering a set of consequences, as auditing firms are reporting back to the FTC on how organizations answer GLBA compliance questions. It's crucial for institutions to be prepared to answer specific questions in GLBA section 314.4 and to have the appropriate measures in place to avoid being in violation of compliance.

UNDERSTANDING GLBA RULES

It's important to not only know the rule language, but also what it means for your organization. Below are detailed excerpts from the GLBA rules along with questions to ask when considering the implications of compliance best practices.

§314.3 STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

INFORMATION SECURITY PROGRAM

(a) You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in §314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

OBJECTIVES

(b) The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

KEY QUESTIONS ABOUT RULE (314.3)

Do you have an information security department at your organization?

Does your information security department have clearly written security policies and procedures?

How do you implement, measure, and maintain your security program?

Have you determined the appropriate safeguards based on your size and IT infrastructure?

Have you identified what sensitive information you're collecting or processing like; PII, HIPAA, or other data?

What attacks or methods of compromise are you anticipating?

Can you properly identify unauthorized access and on what systems?

How do you fix or remediate compromised accounts once they are identified?

How do you validate your security measures?

Do you use any 3rd party penetration testers or GLBA compliance consultants to identify risks and strengths of your organization?

IT'S CRITICAL FOR GLBA COMPLIANCE THAT YOUR ORGANIZATION HAVE AN INFORMATION SECURITY PLAN IN PLACE.

THE PLAN CAN'T BE IN SOMEONE'S HEAD OR FRAGMENTED DOCUMENTS, IT NEEDS TO BE WRITTEN DOWN, ENFORCED, AND MEASURABLE.

§314.4 ELEMENTS

In order to develop, implement, and maintain your information security program, you shall:

(A) Designate an employee or employees to coordinate your information security program.

(B) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(C) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures. Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(D) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

KEY QUESTIONS ABOUT RULE (314.4)

Who is ultimately responsible for item (3) - detecting, preventing, and responding to attacks, intrusion, or other system failures?

Are employees trained and educated on the process of identifying sensitive student information?

Are employees trained to notify the Information Security Program Coordinator if Student PII is compromised?

Does the training program teach employees to recognize and respond to schemes to commit fraud or identity theft?

Are audit logs and logging tools secured or protected from unauthorized access, modification, and deletion?

What tools are you using to capture and maintain logs from necessary sources?

Do you know what sources are necessary to capture logs?

Does IT Operations ensure that equipment removed for off-site maintenance is sanitized of any student PII?

Is media containing student PII sanitized or destroyed before disposal or released for reuse?

Are the identities of users authenticated or verified prior to allowing access to the organization's systems?

How does an employee identify and address compromised accounts?

How is the institution measuring response time on fixing known issues related to PII?

Do you have a risk assessment for all 3 areas, training, information systems, and detection and response?

Does using an MDR provider make sense to help you meet compliance?

Has multi factor authentication (MFA) been enabled for all users that handle PII?

Are secure, locked bins readily available on campus for hard-copy or paper listings of student information when the documents are no longer needed?

Are internal and external vulnerability scans performed on a periodic basis to identify threats and weaknesses?

Are the system security controls periodically assessed to determine if the controls are effective?

WHAT'S AT STAKE?

With so many institutions relying on federal student aid and Title IV funding, there is a lot at stake. A breach or failure to comply with GLBA could result in a loss of necessary funding, fines, reduced enrollment, and loss of reputation. During audits, the Federal Student Aid's Postsecondary Institution Cybersecurity Team (Cybersecurity Team) will be informed of findings related to GLBA, and may request additional documentation from the institution in order to assess the level of risk to student data presented by the institution or servicer's information security system.

If the Cybersecurity Team determines that the institution or servicer poses substantial risk to the security of student information, the Cybersecurity Team may temporarily or permanently disable the institution or servicer's access to the Department's information systems.

Additionally, if the Cybersecurity Team determines that as a result of very serious internal control weaknesses of the general controls over technology that the institution's or servicer's administrative capability is impaired or it has a history of non-compliance, it may refer the institution to the Department's Administrative Actions and Appeals Service Group for consideration of a fine or other appropriate administrative action by the Department.

Under GLBA, penalties for non-compliance can include fines of up to $100,000 per violation, with fines for officers and directors of up to $10,000 per violation. And if that wasn't enough, the provisions include criminal penalties of up to five years in prison, and the revocation of license

BEST PRACTICES

(1) Designating a specific employee with privacy and security management oversight responsibilities

(2) Identifying, in writing, all reasonably foreseeable internal and external risks to security, confidentiality, and integrity of personal information and systems processing personal information;

(3) Designing and implement safeguards, in writing, to control the identified risks;

(4) Training staff to implement the program;

(5) Regularly testing and monitoring the safeguards;

(6) Implementing third party service provider agreements which specify that the third party is maintaining appropriate safeguards; Regularly evaluating and adjusting the program; and

(7) Designing and implementing policies and procedures to respond to incidents involving unauthorized access, disclosure, or use of personal information.

HELPFUL LINKS

HOW COLLEGES AND UNIVERSITIES CAN MAINTAIN GLBA COMPLIANCE

HIGHER EDUCATION REQUIREMENTS FOR GLBA: HOW TO PREPARE FOR AN AUDIT

CYBERSECURITY POLICY FOR TITLE IV ELIGIBILITY

HIGHER ED INSTITUTIONS NEED SIEM SOFTWARE

GLBA CHECKLIST

- Has your college or university assigned an individual on your team to coordinate an information security program?
- Has your institution designated all campus organizations that work with student or parent information in regards to the administration of the FSA program?
- Has your organization created a thorough and efficient process for conducting risk assessments?
- Has your institution conducted a risk assessment in accordance with the guidelines outlined in 16 CFR 314.4(b)?
- Has your college or university created an official document that outlines corrective action for each risk discovered during the risk assessment?
- Has your organization put priority on the most critical risks to your institution and created a corrective action plan?
- Has your institution created reports to show auditors your known risks and safeguards?

THE BITLYFT APPROACH

Our approach to cybersecurity focus on providing our clients with a comprehensive platform that goes beyond MDR, SIEMaaS, and MSSP models. Our team of security experts coupled with our powerful BitLyft AIR platform illuminates and eliminates cyber threats in seconds before they have time to harm you or your customers.

AIR PLATFORM

Visibility
Security Information and Event Management (SIEM)

Expert People
Security Operations Center (SOC)

Speed & Efficiency
Security Orchestration Automation and Response (SOAR)

Intelligence & Accuracy
Central Threat Intelligence (CTI)

The BitLyft AIR platform merges the best of people and software to provide you unparalleled protection for your organization.

LEARN HOW

info@bitlyft.com | www.bitlyft.com | 517.220.0990