GLBA Student Financial Aid Safeguards 2022/2023 Update

ARTICLE 10.19.22 DEAN DORTON

Anyone who hasn't just arrived from the Stone Age recognizes the importance of maintaining a healthy cybersecurity program. Healthy things grow and so our cybersecurity efforts should be adapting to the ever-changing threats that are trying to push our organizations towards extinction.

Doing cybersecurity right isn't cheap. Most colleges and universities have a dinoburger budget and can't afford the brontosaurus ribs. How do you get the resources to protect your systems and data? One way is to communicate that some cybersecurity efforts are required and not doing them can result in loss of grant funding.

The Gramm-Leach-Bliley Act (GLBA) has been around for years, but only had a real impact on colleges and universities for the last 3 to 4 years. Like a cybersecurity program, data security laws have a need to evolve and adapt to changing threats. The standards for the safeguarding components of GLBA have been updated. Some of the updates revise prior rules while others are brand new.

Old Rule	New Rule
Designate the employee(s) responsible for coordinating the information security program.	A single "qualified individual" (QI) is designated to oversee, implement, and enforce the information security program. The QI may be an employee, affiliate, or service provider.
Perform a Risk Assessment	Perform a risk assessment and update it periodically. Risk assessment should include criteria for the evaluation and categorization of identifying risks. This is the use of a cyber security framework. I.E., NIST, ISO, CIS. Risk Assessment should include criteria for the assessment of the confidentiality, integrity, and availability of information including adequacy of existing controls. Risk assessment should include requirements identifying how risks will be mitigated based on the assessment and how the ISP will address risks.
Identify safeguards for each risk identified	Identify safeguards for each risk identified. Safeguards designed should cover – Access controls, Data inventory, Encryption, Secure application development, Multifactor authentication, Secure disposal, Change management and Monitoring and logging user activity Annual penetration testing and vulnerability scanning* Policies and procedures addressing – security awareness training and information security personnel are qualified and trained.

Old Rule	New Rule
	Proper oversight of service providers addressing – selevtion process, contract wording and periodic assessment.
	Have a written incident response plan.*
	QI to prepare and present a written report to the board of directors, at least annually, on the status of the compliance with the information security program. *

There is a new exemption rule for small organizations. If you maintain student financial aid information for less than 5,000 students, some new rules are not required. Rules marked with an asterisk (*) are applicable to the exemption rule.

The date for having these controls in place is December 9, 2022. At a minimum, you should be able to demonstrate the new rules are being met before your next Single Audit is performed in 2023.

Subscribe to Dean Dorton Insights to stay up-to-date with the latest regulatory changes.

Explore IT Audit & Compliance Services

Kevin W. Cornwell, CPA | IT Audit Associate Director
kcornwell@deandorton.com
502.566.1011