Comité de Regulaciones Federales y Estatales – **Boletín 2020-10**

**ELECTRONIC ANNOUNCEMENT**

Esta comunicación recuerda a las Instituciones de sus obligaciones con respecto a proteger la información confidencial de estudiantes y sus padres, conforme a los estándares de la ley GLBA. Cada Institución ha acordado cumplir con estos requisitos dentro de su Program Participation Agreement|PPA. Las Instituciones que no puedan cumplir con estos requisitos podrán ser catalogadas administrativamente incapacitadas. Los resultados de los acontecimientos serán incluidos en el reporte de la auditoría.

ProTEGER esa información es una obligación compartida entre elUSDE, las instituciones, los servicios de terceros| third-party servicers y otros socios en el sistema de ayuda económica. **EL USDE espera que toda las Instituciones mantengan políticas de seguridad sólidas y controles internos efectivos para evitar el acceso no autorizado o la divulgación de información confidencial.**

La Ley Gramm-Leach-Bliley (GLBA), promulgada el 12 de noviembre de 1999, creó el requisito de que las instituciones financieras deben tener ciertas protecciones y salvaguardas de privacidad de la información. La Comisión Federal de Comercio (FTC) tiene autoridad para hacer cumplir los requisitos y ha determinado que las instituciones de educación superior (instituciones) son instituciones financieras bajo GLBA. Cada institución ha acordado cumplir con GLBA en su Acuerdo de Participación del Programa| Program Participation Agreement con el Departamento.

Además, como condición para acceder a los sistemas del USDE, cada institución y administrador debe firmar el Acuerdo de inscripción del Portal de Internet de Ayuda Estudiantil|SAIG, que establece que la institución debe garantizar que toda la información del solicitante de ayuda federal para estudiantes esté protegida contra el acceso o la divulgación al personal no autorizado.

Para información adicional hacer referencia al correo electrónico o número de teléfono al final del anuncio.
The Department of Education (Department) continues to take steps to ensure the confidentiality, security, and integrity of student and parent information related to the federal student aid programs. Protecting that information is a shared obligation among the Department, institutions, third-party servicers, and other partners in the financial aid system. We expect all of our partners to maintain strong security policies and effective internal controls to prevent unauthorized access or disclosure of sensitive information.

The Gramm-Leach-Bliley Act (GLBA), which was signed into law on November 12, 1999, created a requirement that financial institutions must have certain information privacy protections and safeguards in place. The Federal Trade Commission (FTC) has enforcement authority for the requirements and has determined that institutions of higher education (institutions) are financial institutions under GLBA.

Each institution has agreed to comply with GLBA in its Program Participation Agreement with the Department. In addition, as a condition of accessing the Department’s systems, each institution and servicer must sign the Student Aid Internet Gateway (SAIG) Enrollment Agreement, which states that the institution must ensure that all federal student aid applicant information is protected from access by or disclosure to unauthorized personnel.

Institutions and third-party servicers are also required to demonstrate administrative capability in accordance with 34 C.F.R. § 668.16, including the maintenance of adequate checks and balances in their systems of internal control. An institution or servicer that does not maintain adequate internal controls over the security of student information may not be considered administratively capable.

In Dear Colleague Letter GEN-15-18 and GEN-16-12, we reminded institutions about the longstanding requirements of GLBA and notified them of our intention to begin enforcing legal requirements of GLBA through annual compliance audits. In Dear CPA Letter CPA-19-01, we explained the procedures for auditors to determine whether institutions were in compliance with GLBA. This announcement explains the Department’s procedures for enforcing those requirements and the potential consequences for institutions or servicers that fail to comply.

Audit Findings

Auditors are expected to evaluate three information safeguard requirements of GLBA in audits of postsecondary institutions or third-party servicers under the regulations in 16 C.F.R. Part 314:

1. The institution must designate an individual to coordinate its information security program.

2. The institution must perform a risk assessment that addresses three required areas described in 16 C.F.R. 314.4(b):

   a) Employee training and management;
b) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

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

3. The institution must document a safeguard for each risk identified in Step 2 above.

When an auditor determines that an institution or servicer has failed to comply with any of these GLBA requirements, the finding will be included in the institution’s audit report.

Federal Trade Commission

When an audit report that includes a GLBA audit finding is received by the Department, we will refer the audit to the FTC. Once the finding is referred to the FTC, that finding will be considered closed for the Department’s audit tracking purposes. The FTC will determine what action may be needed as a result of the GLBA audit finding.

Cybersecurity Team

Federal Student Aid’s Postsecondary Institution Cybersecurity Team (Cybersecurity Team) will also 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.

Contact

If you have questions about the Department’s enforcement of the GLBA, please contact the Cybersecurity Team at fsaschoolcybersafety@ed.gov or by phone at 202-245-6550.

We recognize the substantial investments in time and resources that institutions and servicers have devoted to protection of student data and we thank our partners for their willingness to address evolving cybersecurity threats.

COMITÉ DE REGULACIONES FEDERALES Y ESTATALES