GLBA - Updated Safeguards Rule Compliance

STUDENT FINANCIAL AID INFORMATION

Carlos S. Lobato, CISO
Robert Doyle, CPO and IT Compliance Officer
Information Technology

BE BOLD. Shape the Future.
New Mexico State University
Overview of GLBA /Institutional Responsibilities

• What is GLBA?
• Why is NMSU treated as a Financial Institution under GLBA?
• What are the consequences for GLBA non-compliance?
• Responsibilities of the NMSU system
  • Presidents and CIOs
  • CISO designated qualified individual
    • Annual Written Report to the Governing Board
  • Financial Aid Director and Staff
• Protection of Student Financial Aid Information
  • GLBA’s Safeguards Rule
    • Cybersecurity Requirements
  • GLBA’s Privacy Rule
• NMSU Policy and Resource
• Q & A
What is GLBA?

The Gramm-Leach-Bliley Act (GLBA) is a federal law in the US that requires financial institutions to protect the privacy of their customers' personal information.

GLBA also requires institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.

At NMSU, students are considered our customers for GLBA purposes.
NMSU is a Financial Institution under GLBA

The GLBA defines financial institutions as organizations that are significantly engaged in providing financial products and services. Title IV institutions are deemed financial institutions per GLBA due to financial services provided, including payment plans and student loans, and are required by the Federal Student Aid (FSA) Program Participation Agreement (PPA) and the Student Aid Internet Gateway (SAIG) Agreement to have sufficient GLBA safeguards in place (Safeguards Rule – Details Cybersecurity Requirements).
Consequences for GLBA Non-Compliance

Failure to comply can include both monetary fines and/or imprisonment:

• Civil penalties of up to $100,000 for each violation
• Fines of up to $10,000 per violation for officers and directors of an institution
• The largest penalty for non-compliance would be the risk of restricted or loss of Title IV funding, and ineligibility to participate in federally funded financial aid programs.
• Intangible costs include the loss of customer confidence, lost productivity, and the reputational damage that follows.
• In higher education, reputational damage is harder to quantify, but can still be seen over time through changes in enrollment numbers, decreased donor contributions, and decreased spending on campus.

It is essential for financial institutions to comply with the GLBA and associated Safeguards Rule and take appropriate measures to safeguard sensitive information and maintain customer trust.
Responsibility of NMSU system

Note: Financial Aid Funding at risk if not compliant
Responsibility of NMSU system

3. The Institution agrees to comply with --
   a. Title VI of the Civil Rights Act of 1964, as amended, and the implementing
      regulations, 34 C.F.R. Parts 100 and 101 (barring discrimination on the basis of race,
      color or national origin);
   b. Title IX of the Education Amendments of 1972 and the implementing regulations, 34
      C.F.R. Part 106 (barring discrimination on the basis of sex);

Note: Compliance requirement with FERPA and GLBA


PPA. OPE ID: 00265700. PPA Expiration Date: 06/30/2022
Page 3 of 18
Responsibility of NMSU system

The GLBA requires institutions to, among other things:

- Develop, implement, and maintain a written information security program;
- Designate the employee(s) responsible for coordinating the information security program;
- Identify and assess risks to customer information;
- Design and implement an information safeguards program;
- Select appropriate service providers that are capable of maintaining appropriate safeguards; and
- Periodically evaluate and update their security program.

Source: Dear Colleague Letter from US Department of Education
Responsibility of NMSU system

Under these GLBA requirements, Presidents and Chief Information Officers of institutions should have, at a minimum, evaluated and documented their current security posture against the requirements of GLBA and have taken immediate action to remediate any identified deficiencies.

Finally, we also are informing institutions that the Department is beginning the process of incorporating the GLBA security controls into the Annual Audit Guide in order to assess and confirm institutions’ compliance with the GLBA. The Department will require the examination of evidence of GLBA compliance as part of institutions’ annual student aid compliance audit.

Source: Dear Colleague Letter from US Department of Education
Responsibility of NMSU system

CISO Designated Qualified Individual

• Annual Written Report to the Governing Board
• CPO and IT Compliance Officer
  • Verifies and Confirms Compliance
  • Advisor to CISO
• Financial Aid Director and Staff
  • Receive, process, and handle Student Financial Information
  • Store and safeguard Student Financial Information
  • Follow and implement administrative, technical and physical controls
  • Knowledgeable of safe computing and data security practices
  • Knowledgeable of general access controls and NMSU policies
  • Take NMSU’s computer, privacy & data security trainings and others as appropriate
Protection of Student Information

The revised Safeguards Rule provides more detailed guidance on the security requirements organizations need to implement in order to be compliant. The FTC identified the following elements under the Rule:

- Written Information Security Program
- Designation of a Qualified Individual
- Periodic Risk Assessments
- Testing and Monitoring
- Employee Training
- Vendor Management
- Evaluation of the Information Security Program
- Incident Response Plan
- Annual Board Reports
DEFINING GLBA SCOPE FOR HIGHER ED

What is in scope?

• Any people, processes, or technologies that store, process or transmit NPI.
• Any systems connected to systems that store customer information.
• Include servers and workstations, firewalls, student information systems, departments accessing NPI, file cabinets, paper documents, or media with NPI.

What information is in scope?

• All Non-public Personal Information (NPI) that a consumer provides to obtain a financial service or product.
• Any customer NPI stored, transmitted, or processed as part of GLBA-covered services.
• Includes: Social Security Numbers, credit card numbers, financial statements and balances, loan applications, credit history, health information, account numbers, National IDs.
DEFINING GLBA SCOPE FOR HIGHER ED

When is this information collected?

- Servicing student loans or financial aid
- Federal work study
- Extending credit for tuition, fees, housing or medical services
- Financial advisory services (401k programs)
- Debt collections
- Check cashing services
- Career counseling services
- Health insurance provisioning, etc.
DEFINING GLBA SCOPE FOR HIGHER ED

Commonly Impacted Departments:

• Financial Aid
• Admissions/Enrollment
• Registrar
• Bursar
• Student Loans
• Student Services
• Housing
• Institutional Research
• Fundraising (Development, Foundation, Alumni), etc.
INFORMATION SECURITY PROGRAM REQUIREMENTS

1. At a minimum, the written information security program must address the implementation of the minimum safeguards identified in 16 C.F.R. 314.4(c)(1) through (8). Previous communications from the Department of Education referenced use of the NIST SP 800-171 for outlined safeguards and security controls.

2. Access control and limiting access only to authorized users and the information they need to perform their duties and functions. Organizations must review access on a regular basis.

3. Keeping an up-to-date inventory. Identifying and managing the data, personnel, devices, systems, and facilities involved. It is impossible to protect sensitive information if you don’t know where it is located.
INFORMATION SECURITY PROGRAM REQUIREMENTS

4. Encrypting all customer information in transit over external networks and at rest.
5. Adopting secure development practices for any applications in use (both in-house and outsourced systems).
6. Implementing Multi-factor Authentication for any individual accessing any information system that contains customer information.
7. Administering procedures for secure disposal no later than two years after the last date the information is used unless retention is necessary for a legitimate business purpose.
8. Adopting procedures for change management – documented procedures to assess the security of devices, networks, or other systems added or removed from the environment.
9. Reinforcing procedures and controls to monitor and log the activity of authorized users and detect unauthorized access.
GLBA: BEST PRACTICES FOR PROTECTING INFORMATION

- Securely destroy paper and computer files containing Non-public Personal Information (NPI), following NMSU RMR requirements.
- Secure all stored NPI in a locked desk or file cabinet (do not keep files on your desk!).
- Never click on links or attachments in suspicious emails.
- Do not utilize personal laptops or phones for accessing systems containing NPI.
- Do not use unsecured messaging channels like email, text, etc. to transmit NPI.
- Do not share accounts with other users.
- Recognize and report suspicious activities immediately.
- Collect only what you need. Keep it safe. Dispose of it securely.
GLBA: PRIVACY RULE

NOTE:
It has been determined that if an institution is FERPA compliant that then the institution is compliant with the GLBA Privacy Rule.

NMSU is compliant with FERPA.
NMSU Policies and Resources

- Publicly Available Policy: 15.63 – Protection of Customer Information; GLBA Compliance
- Internal website: https://inside.nmsu.edu/glba/
- CISO is the Responsible Administrator
- CIO, IT Compliance and CISO will handle Data Breaches
- CPO and CISO available to answer questions
Contact Information

Carlos S. Lobato, CISO
Robert Doyle, CPO and IT Compliance Officer
Information Technology

575-646-5902, 575-646-5969 or Teams [preferred]
clobato@nmsu.edu and rdoyle@nmsu.edu
References:

- U.S. Department of Education’s Dear Colleague Letters
- Federal Trade Commission (FTC) GLBA website
- Rapid7 GLBA guidance
- CampusGuard GLBA guidance