GLBA COMPLIANCE CHECKLIST

What are the first steps your organization can take toward GLBA Compliance?

- [ ] Appoint a designated, qualified individual.

- [ ] Complete an inventory of all systems/applications used to access, store, or transmit NPI data.
  - [ ] List of all staff/student employees with access to NPI.
  - [ ] Inventory of what information/data is collected and why/purpose.
  - [ ] How information is collected and details around process for each method (in-person, online, phone, fax, email, mail, campus mail).

- [ ] Review procedures for accessing identified systems (access controls, password/MFA requirements, etc.).

- [ ] Analyze remote procedures if the process is different when accessing any systems or applications from home/hybrid work environments.

GLBA COMPLIANCE CHECKLIST

- [ ] Examine procedures for data storage, including physical security controls for any paper-based data, and where data is stored electronically (data retention and data destruction/disposal).
- [ ] Review incident response procedures – the process in the event of a suspected or confirmed data compromise.
- [ ] Reduce scope as much as possible, and eliminate all storage, transmission, and access to NPI anywhere you can.
- [ ] Segment NPI systems from the internet and other relatively open networks.
- [ ] Design a robust information security program to protect these systems.
- [ ] Determine safeguards for systems based on risk.
- [ ] Train employees to improve awareness.
- [ ] Evaluate the compliance and security of all third-party service providers.