Information Security Laws and Regulations

Federal:

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Financial Services Modernization Act of 1999, or Gramm Leach Bliley Act (GLB)

State:

- Georgia Computer Systems Protection Act

Family Educational Rights and Privacy Act (FERPA)

FERPA, by far the most significant federal law for educational institutions, deals with student “education records,” defined to mean (with a few exceptions) records containing information directly related to a student that are maintained by a school or its agent. “Education records” is broadly defined and includes electronic records. FERPA prohibits schools from disclosing education records, or personally identifiable information in those records other than certain basic “directory information,” without the student's prior written consent unless an exception applies. FERPA states that:

- Neither the full nor partial SSN may be used to post grades to a course website; neither may a general university issued student ID number. An ID number specifically issued for the posting of grades, and no other purpose, may be used.
- A unique, university issued ID may be designated and disclosed as directory information IF it cannot be used, on its own, to access non-directory personal information.
- An institution that allows a student or third party to access education records by providing only publicly available information, such as a name or email address, without additional authentication of identity, may have a “policy or practice” in violation of FERPA because it could text-lg to the unauthorized disclosure of education records.

See CSU ID for details on compliance at CSU.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA deals with the protection of personally identifiable information relating to health care. HIPAA applies to “covered entities,” which includes health care providers who transmit information in electronic form in connection with certain standard transactions (generally related to billing). Many institutions of higher education contain units that are covered entities, and some institutions are covered entities in their entirety. The requirements of HIPAA apply only to those portions of an institution that constitute a “covered entity.” Nevertheless, those requirements may spill over effectively to other operations within an institution, depending on the degree of centralization and uniformity of its information technologies operations and policies, and the extent to which the HIPAA requirements are seen as supplying “best practices” for data protection.

In brief, HIPAA has two rules. The Privacy Rule determines what data is considered “protected health information” (information that relates to a past, present or future medical condition, health care treatment, or coverage of the individual) and who may have access to it. The Security Rule focuses on ensuring that only those who are authorized actually do have access.

See the Confidentiality site for details on compliance at CSU.

Gramm Leach Bliley Act (GLBA)

The Gramm Leach Bliley Act (GLB) requires that financial institutions safeguard nonpublic customer data, limit disclosures of such data, and notify customers of their information sharing practices and privacy policies. Because higher education institutions generally participate in a substantial amount of lending activity (and may engage in other covered activities as well), the FTC considers them covered financial institutions.

The act states, among other things, that institutions must develop, implement and maintain a written comprehensive information security program that contains administrative, technical, and physical safeguards appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the relevant customer data. The plan must be “reasonably designed” to achieve the security and confidentiality of customer data, to protect against anticipated threats or hazards, and to protect against unauthorized access or use that could result in substantial harm.

CSU's Information Security Officer is responsible for developing, implementing, and maintaining a written comprehensive information security program.

Georgia Computer Systems Protection Act

The Georgia Computer Systems Protection Act, (“GCSPA”), O.C.G.A. § 16-9-90, provides that any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than $50,000.00 or imprisoned not more than 15 years, or both.