Harding University Information Privacy and Security Program

The Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA) contain regulations that govern the conduct of university officials with access to nonpublic personal information (NPI) of stakeholders. These regulations apply to nonpublic personal information in any format (i.e., electronic, print, handwritten, etc.).

For the purposes of this document, a *stakeholder* is defined to include all students, parents, alumni and donors, as well as other individuals "doing business" with the university. *Nonpublic personal information* is defined to be any personally identifiable information, or list, description or grouping of stakeholders that is derived using any personally identifiable information that is not publicly available. A *university official* is defined to be anyone with official university permission to access stakeholder information. This includes but is not limited to board members, administrators, faculty members, staff and preceptors, as well as any graduate assistants and student workers who have access to stakeholder information.

The University has policies in place such as the Computer Use Policy, IT Resource Policy, and Privacy Policy (which includes regulations from FERPA, HIPAA and GLBA) to ensure the privacy and protection of all nonpublic personal information obtained, created or maintained by university employees. Stakeholders are made aware of these policies, and they are also all available, as well as information on FERPA, GBLA and HIPAA, on the university web site at www.harding.edu/ConsumerInfo.

The University is committed to maintaining the security, integrity, and confidentiality of all nonpublic personal information, and so it requires that all University officials be aware of and abide by applicable federal, state and university regulations. All university officials are required to sign a Computer Users Agreement which commits them to follow these and other university policies before gaining access to the university's computer systems and network.

Designated Program Coordinators

The Information Privacy and Security Committee (IPSC) is responsible for the coordination and oversight of the Information Privacy and Security Program. The committee is comprised of a key administrator from each of the following areas or offices: Academic Affairs, Business, Financial Aid, Information Systems and Technology (IS&T), Registrar, and Student Life. Any question about policy or procedures related to privacy or security of stakeholder information should be emailed to ConsumerInfo@harding.edu.

Privacy Policy

Harding University publishes a privacy policy at www.harding.edu/ConsumerInfo. This is a comprehensive policy intended to cover all privacy issues at the university, including those regulated by FERPA, GLBA and HIPPA. It contains a clear statement of the university's privacy practices, and includes a description of the type of stakeholder information that is collected and shared, with whom it is shared, and how the integrity and confidentiality is safeguarded.

The university collects and maintains stakeholder information, and university officials must access this information to carry out their responsibilities for official university business. University officials with a "legitimate need to know" will have access to nonpublic personal information of stakeholders. The definition of "legitimate need to know" for a university official is that the information is required in order to complete their assigned duties for the university. Examples of "legitimate need to know" include:

1. Perform an administrative task outlined in the official's position, description or contract approved by the University board of trustees;
2. Perform a supervisory or instructional task directly related to the student's education;
3. Perform a service or benefit for the Student such as health care, counseling, job placement or financial aid; or
4. Perform a task relating to athletic conference compliance, rules and regulations.

University officials cannot use or disclose nonpublic personal information without the stakeholder's prior written consent, except for in "legitimate need to know" situations. University officials cannot release any stakeholder information to individuals or organizations not associated with the university. Requests for stakeholder information from anyone not associated with the university must be emailed to ConsumerInfo@harding.edu.

The University designates the following nonpublic personal information as "directory information" in order that the University may, at its discretion, disclose the information without a student's prior written consent: name, campus address, permanent address telephone number, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees, achievements, academic awards, honors, most recent previous educational agency or institution attended, social clubs, academic clubs and societies. In addition to these items, by enrolling at the University, the student consents to allowing the University to photograph her or him for promotional and identification purposes.

A student has the right to further restrict the release of directory information if he or she chooses to do so. He or she must notify the FERPA administrator in writing in order to prevent disclosure of specific directory information. Questions about this can be directed to the University's FERPA administrator by email at registrar@harding.edu

Risk Assessment

The IPSC committee is responsible for collecting information on internal and external risks to the integrity, privacy and security of stakeholder information. Members of the committee are administrators specifically selected from areas and offices on campus with a high level of involvement with stakeholder information. The committee will communicate regularly about risks and the university response to those risks. Any member of the committee can call a meeting to address concerns that a risk is not being appropriately addressed.

Electronic access to information creates many opportunity for internal and external risks. The IS&T representative on the IPSC committee represents the needs and interests of the IPSC committee in the bi-weekly IS&T operations meetings. In these meetings, internal and external risks to the integrity, security and confidentiality of all electronic information on campus are discussed, as well as the appropriate response of the university to protect against these risks. Details from this meeting will be reported back to the IPSC committee each month via email, so the committee members can determine if additional action is required.

The Student Life member of the IPSC committee is responsible for staying current on issues related to HIPAA regulations. The Harding University Registrar is responsible for FERPA regulations.

The Financial Aid member of the IPSC committee is responsible for evaluating and reporting to the committee the safeguards that are in place for service providers who use nonpublic personal information to provide a service to stakeholders. Examples of such service providers for the university are ECSI and private lenders.

Training

All university officials are required to be aware of and abide by university privacy and security policies, and must sign a Computer Users Agreement before gaining access to the university's computer systems and network. New Users are required to read the policies related to privacy and security and also receive training on privacy and security from the Departments of Human Resources and the Department of Information System and Technology, as well as from their immediate supervisor. Training modules are being developed in Moodle (an online course management system) which will be used to provide ongoing training to all university officials.