Rice University Policy No. 808

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

General Policy

Rice University complies with Federal, State and local laws and regulations related to the protection of confidential or sensitive personally identifiable information in conducting university business. Personally identifiable information is data which is tied to, or otherwise enables identification of, a specific person and makes personal information about them known.

This policy covers students, employees, donors, alumni, prospects, applicants, research subjects, and others on whom the university may have such information. The policy applies regardless of how the information is stored (e.g., paper, electronic, other media) or transmitted.

Definitions

Confidential Information. University personnel should treat as "Confidential Information" personally identifiable information deemed confidential by law, regulation or University policy or which contains information that is highly private or personal or could lead to identity theft if mishandled. Confidential information includes the following specific information:

1. Social security numbers
2. Credit card numbers
3. Driver's license or other government-issued identification numbers
4. Bank account information
5. Protected health information
6. Student education records (including grades and disciplinary records)

Examples of where this confidential information is located include:

1. Financial Records (e.g., employee loans; donor financial information; student and family financial information including tax returns; payroll records).

2. Health Records (e.g., employee benefit plan information; workers compensation claim information; student medical records; student counseling center information; information regarding disabilities).

Use and release of any such confidential information shall be consistent with law and University policy.

Sensitive Information. Some information related to Rice's business and academic activities, although not cloaked with the same level of concern or legal protection as confidential information, is still considered by Rice to be "sensitive information". Examples of these types of information include, but are not limited to:

1. Birth dates
2. Home addresses
3. Emergency contact information
4. Employee ID numbers
5. Employee disciplinary records
6. Legal documents (unless publicly disclosed by the University)
7. Financial records (unless publicly disclosed by the University)
8. Infrastructure information (e.g., IT, physical plant) (unless publicly disclosed by the University)

Organizational units must be mindful that while some information may be directory information that would not ordinarily be confidential or sensitive, there may be other reasons for not disclosing the information (e.g., if a student has requested the Registrar not release directory information about that student).

Elaboration of Policy

Information deemed confidential or sensitive should be collected, stored, transmitted and disposed of using the following guidelines. Each organizational unit of the university is responsible for ensuring that confidential/sensitive information is:

1. Collected only as necessary in conjunction with academic and business needs.

2. Restricted in its distribution and accessibility (in some cases approved by a supervisor) as is consistent with good internal control practices, with employees with access to such information being informed of applicable restrictions.

3. Properly secured by the use of such safeguards as secured file storage and rooms, encryption, and other technology tools.

4. Disposed of through secure means such as shredding and thoroughly erasing hard drives.

Confidential and sensitive information should be shared internally only on a need-to-know basis and externally only consistent with law, business and educational necessity and adequate protections, which should include written confidentiality agreements if appropriate. If shared internally, colleagues should be informed of the confidential or sensitive nature of the information and the need to safeguard it. If there is any doubt about the appropriateness or prudence of disclosing personally identifiable information, the unit should confer with the Office of General Counsel, Office of Human Resources (for employees) or the Office of the Registrar (for students).

Responsible Offices

1. The designated Rice University Information Security Officer provides tools, services, and guidance related to the security of the university's information technology assets. Questions related to these services, as well as questions related to the theft or potential theft of personally identifiable information, should be directed to the Information Security Officer.

2. The Office of General Counsel provides legal guidance for questions related to the treatment of confidential or sensitive information, including: educational records under FERPA; medical or health-related information under HIPAA, the ADA or FMLA; financial information of customers of the university under the GLBA; and credit card information obtained and/or maintained under the PCI-DSS.

/s/ David W. Leebron
David W. Leebron
President

Policy No. 808

Adopted: February 17, 2011

Appendix to Policy No. 808– Various Laws and Regulations relating to Personally Identifiable Information

1. **FERPA—Family Educational Rights and Privacy Act.** Limits the disclosure of "education records" defined as those records that are: (a) "directly related" to a student, and, (b) maintained by or on behalf of the university.
   a. A record is "directly related" to a student if it is "personally identifiable" to the student.
   b. A record is "personally identifiable" to a student if it expressly identifies the student by name, address, birth date, social security number, ID number, or other such common identifier.
   c. Examples of "education records" at Rice include registrar records, transcripts, papers, exams, individual class schedules, financial aid records, financial account records, disability accommodation records, disciplinary records, placement records.
   d. "Education records" do not include directory information, unless the student has elected to block the release of directory information.
   e. "Directory information" at Rice includes a student's name, residential addresses, telephone numbers, electronic addresses, date and place of birth, fields of study, dates of attendance, degrees and awards, participation in recognized activities, weight and height of athletic team members, most recent prior educational institution, and a photographic image.
   f. "Education records" also generally do not include certain police records, employment records, health records, or personal memory aid records. Such records may be subject to other regulatory or University policy restrictions.

2. **HIPAA—Health Insurance Portability and Accountability Act.** Imposes privacy and security standards addressing the use, disclosure, storage and transfer of "protected health information".
   a. "Protected health information" means "individually identifiable health information," which is any information that identifies an individual and relates to the individual's:
      i. Past, present or future physical or mental health or condition,
      ii. Provision of health care, or
      iii. Past, present, or future payment for the provision of health care.
   b. Information is deemed to identify an individual if it could enable someone to determine the individual's identity, such as through an identifier or characteristic that could uniquely identify the individual.
   c. Common identifiers that will make health information "individually identifiable" and therefore deemed "protected health information" include name, address, birth date, social security number, ID number, or other such common identifier.
   d. Examples of information that should be treated as "protected health information" at Rice include employee benefit plan information, worker's compensation claim information, student health services information and student counseling center information.

3. **GLB—Gramm-Leach-Bliley Act.** Requires implementation of a written information security program for "customer information."
    a. "Customer information" means any record containing "nonpublic personal information" handled or maintained by or on behalf of the institution about a customer of that institution.
    b. "Nonpublic personal information" includes "personally identifiable information," which in turn is defined as any information:
        i. a customer provides to obtain a financial product or service from the institution,
        ii. about a customer resulting from any transaction with the institution involving a financial product or service, or
        iii. otherwise obtained about a customer in connection with providing a financial product or service to that customer.
    c. Common identifiers that will make financial information "personally identifiable" and therefore deemed "customer information" include name, address, birth date, social security number, ID number, or other such common identifier.
    d. Examples of "customer information" at Rice include financial records of employees (such as loans), students and their parents (such as cashier's accounts or information related to financial aid), and donors.

4. **PCI-DSS –Payment Card Industry Data Security Standards.** Requires implementation of security standards surrounding the authorization, processing, storage, and transmission of credit card data. The security standards apply to electronic and paper credit card data.
    a. "Credit card data," as defined by PCI-DSS, is the first six and/or the last four digits of any credit card provided by a customer to conduct University business. If all digits of the credit card are used in the conduct of University business, then name, card expiration date, and source code are considered "credit card data"; and, hence, must be protected.
    b. Examples of operations where PCI-DSS occur on campus include, but are not limited to, Resource Development, Parking, the Glasscock School of Continuing Studies, the Jones Graduate School of Business, the Fondren Library, and the Shepherd School of Music, among others, as well as various events and functions for which credit card payments are taken.

5. **Texas Identity Theft Enforcement and Protection Act.** Requires implementation and maintenance of reasonable procedures to protect information collected or maintained in the regular course of business from unlawful use or disclosure. This includes:
    a. an individual's first name or first initial and last name in combination with at least one of the following identifiers (if the name and the identifier(s) are not encrypted): social security number, driver's license number, government identification number, account number or credit or debit card number along with any required access code; or
    b. information that identifies an individual and relates to the individual's:
        i. physical or mental health or condition,
        ii. provision of health care, or

iii. payment for the provision of health care.

c. Publicly available information from federal, state, or local governments is not covered

6. **Federal Freedom of Information Act or to the Texas Open Records Act.** As a private institution, Rice is not subject to the Federal Freedom of Information Act or the Texas Open Records Act.