



Personal Information Protection (PIP) Policy

Title: Data Classification Policy

Approved: March 4, 2008

Author: Personal Information Risk Group (PIRG)

Version: 1.0

Scope

This policy covers all data produced, collected or used by Loyola University Chicago, its employees, student workers, consultants or agents during the course of University business.

Purpose

The purpose of this policy is to identify the different types of data, to provide guidelines and examples for each type of data, and to establish the default classification for data.

Policy

Data Classification Types

All data covered by the Scope of this policy will be classified as Loyola Protected data, Loyola Sensitive data, or Loyola Public data.

Loyola Protected data

Loyola Protected data is any data that contains personally identifiable information concerning any individual and is regulated by local, state, or Federal privacy regulations, or by any voluntary industry standards or best practices concerning protection of personally identifiable information that Loyola chooses to follow.

These regulations may include, but are not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Illinois Personal Information Protection Act
- Payment Card Industry Data Security Standards (PCI DSS)

Examples of some of the types of data that are regulated are listed in the appendix.

Loyola Sensitive data

Loyola Sensitive data is any data that is not classified as Loyola Protected data, but which is information that Loyola would not distribute to the general public.

This classification is made by the department originating the data. Examples of the types of data included are: budgets, salary and raise information, and possible properties for Loyola to purchase.

Loyola Public data

Loyola Public data is any data that Loyola is comfortable distributing to the general public. For department-specific data, this classification comes from the department. If data is created jointly by more than one department, the involved departments should jointly classify the data. If they are unable to come to a consensus, then the data must be classified as Loyola Sensitive Data. For University-wide data, this classification can only come from the Office of the President, the Office of Registration and Records, the Division of Academic Affairs, or Institutional Research. Examples of the types of data included are: department faculty lists, department addresses, press releases, and the Loyola web site. Any Loyola data that does not contain personally identifiable information concerning any individual, and that is not Loyola Protected data or Loyola Sensitive data, must be classified as Loyola Public data.

Default classification of data

Any data that contains personally identifiable information concerning any individual or that is covered by local, state, or Federal regulations, or by any voluntary industry standards concerning protection of personally identifiable information that Loyola chooses to follow, is automatically classified as Loyola Protected Data. All other data is classified as Loyola Sensitive Data by default. Online resources will be available to assist individuals in properly classifying data.

Questions about this policy

If you have questions about this policy, please contact the Information Security team at DataSecurity@luc.edu.

Appendix

Loyola Protected Data

Listed below are examples of types of personally identifiable information that are generally protected by local, state, or Federal privacy regulations. These examples are not an exhaustive list of all possible types of information that are protected by local, state, or Federal privacy regulations.

Examples:

- Social security numbers
- Credit card and debit card numbers
- Bank account numbers and routing information
- Driver's license numbers and state identification card numbers
- Student education records
 - **Bursar's Office:** Student account files and Perkins loan information
 - **Departments and Colleges:** Academic advising records, admission files, including ACT, SAT and TOEFL scores, and high school and college transcripts and other scholastic records
 - **Directory Information:**
 - Name
 - Address(es) and telephone number
 - University e-mail address
 - Photograph
 - Major and minor field(s) of study, including the college, division, department, institute or program in which the student is enrolled
 - Dates of attendance
 - Grade level (such as freshman, sophomore, junior, senior or graduate level)
 - Enrollment status (undergraduate or graduate, full-time or part-time)
 - Date of graduation
 - Degree(s) received
 - Honors or awards received, including selection to a dean's list or honorary organization Name
 - Participation in officially recognized activities or sports
 - University e-mail address
 - Weight and height of members of athletic teams
 - **Financial Assistance:** Financial assistance application files, student federal work-study information, scholarships and Stafford loan information
 - **Intercollegiate Athletics:** Injury reports, scholarship contacts, performance records, height and weight information

- **Registration and Records:** Permanent record of academic performance (grades, transcript, including supporting documents), course schedules
- **Residence Life:** Residential life and housing services files
- **Student Life:** Student activity files, student disciplinary files, multi-cultural programs and services files, and intramural sports files
- **Student Services:** Career planning files, including placement information and employers' files, international programs and services files
- **Undergraduate Admission and other admission offices:** Admission files on prospective students
- **University Library:** Circulation records
- Personal health records
 - **Patient information:** addresses, dates, telephone/fax numbers, social security numbers, medical records numbers, patient account numbers, insurance plan numbers, vehicle information, license numbers, medical equipment numbers, photographs, fingerprints, e-mail and Internet addresses
 - **Note:** Personal health records stored in education records are subject to FERPA and are excluded from HIPAA.

Additional Information about referenced regulations

FERPA

FERPA is a Federal law that protects the privacy of student education records. This law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA provides students with the right to inspect and review certain education records maintained by the school and to request corrections if the records are inaccurate or misleading. It requires that schools obtain written permission before releasing information from a student's education record. It also allows schools to publish certain "directory" information about students, unless the student has requested that the school not do so.

The penalty for failing to comply with FERPA is loss of all federal funding, including grants and financial aid.

Additional information can be found at

<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html> and at <http://www.luc.edu/ferpa> .

GLBA

GLBA protects consumers' personal financial information held by financial institutions. It requires that financial institutions provide customers with a

privacy notice explaining what information is collected, how it is used, and how it is protected.

The penalty for failing to comply with GLBA is a fine of up to \$100,000 for the institution and of up to \$10,000 for the officers and directors of the institution.

Additional information can be found at <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html> .

HIPAA

HIPAA protects the privacy of Protected Health Information (PHI). It establishes regulations for the use and disclosure of PHI, including a patient's health status, provision of health care, medical records or payment history.

Penalties for wrongfully disclosing PHI range from a \$50,000 to a \$250,000 fine and a one year to a ten year prison term, depending on the circumstances. These fines are for the individual, not the institution.

Additional information can be found at <http://www.hhs.gov/ocr/hipaa/> .

Illinois Personal Information Protection Act

This law protects the personal information of Illinois residents. It requires that an institution which houses social security numbers, driver's license numbers, state ID numbers, bank account numbers and/or credit card numbers provide consumers with notice of any security breaches that compromise that information.

A violation of this act is a violation of the Illinois Consumer Fraud and Deceptive Practices Act and could result in civil money penalties.

Additional information can be found at <http://www.ilga.gov/legislation/94/HB/PDF/09400HB1633lv.pdf> .

Payment Card Industry Data Security Standards (PCI DSS)

PCI DSS is an industry standard which protects credit card customer account data. It requires specific control objectives be met by any organization that accepts credit cards for payment. These control objectives include secure network, server, and desktop standards, as well as procedures to ensure that credit card data is properly protected during the transaction.

Failing to comply with PCI DSS can result in significant fines. Credit card providers can fine merchants up to \$500,000 per compromise when the merchant was not compliant at the time of the compromise. Merchants may also be banned from accepting certain types of credit cards.

Additional information can be found at
<https://www.pcisecuritystandards.org/tech/index.htm> .

Additional US State Laws

If you work for Loyola inside the United States but outside of Illinois, please send an email containing the state in which you work to DataSecurity@luc.edu. The Information Security team will respond to you with any data privacy laws that also apply to you.