UM Policies: Miscellaneous

Last Update: 10 August 2012

DCIE - Personal Identification Information Policy

Purpose
This procedure aims at safeguarding personal identification information of students, employees and other parties.

Policy
Personally identifiable information (PII) is “any information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible sources.” “It includes information that is linked or linkable to an individual, such as educational, financial and employment information.”

Safeguarding university-held PII (and other sensitive information) is the responsibility of each and every member of the University's workforce. Regardless of the role, every employee should be aware of what PII is and act responsibility to ensure its protection.

Examples of information that may be considered PII are:

I. Name, such as full name, maiden name, mother's maiden name, or alias;
II. Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, and financial account (check routing number) or credit card number;
III. Address information, such as street address or email address;
IV. Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people;
V. Telephone numbers, including mobile, business, and personal numbers;
VI. Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), template data (e.g. voice signature);
VII. Information about an individual that is linked or linkable to one of the above (e.g. date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, education information, financial information).

Sometimes, one or two pieces of information can be combined with other information to compromise someone's identity, even if the individual pieces of information seem harmless.
General guidelines to safeguard PII data are summarized below:

I. Printed reports with PII data should identify the name of the individual responsible for printing as well as the date/time and data source.
II. Supervisors and managers are responsible for supervision of employees who have the ability to print such reports.
III. Avoid printing Social Security numbers unless required by law or absolutely necessary to meet a business-related need.
IV. Always store paper reports containing PII in a secure location such as a locked filing cabinet.
V. Shred paper with PII before discarding.
VI. Limit distribution of documents with PII.
VII. Physical access controls should be used for offices or any other area that houses records with PII.

In reference to the storage of PII data, the Division of Continuing and International Education practice is to secure the documents in locked file cabinets whose access is granted by the department supervisor to his/her designee.

A locked storage room has been designed for some of PII paper records containing first and last name of students, financial records, credit card information and it is located in Allen Hall, first floor. Access to the room is granted via a key provided to the Sr. Admin Assistant and the Registrar. Access to the cabinet is granted by the Sr. Admin Assistant.

Requests for non-credit certificates are maintained in a locked cabinet whose key is kept by the Sr. Admin Assistant who also releases the certificates.

Office of HIPAA Privacy & Security