

PII- Personally Identifiable Information-Training and Fraud Prevention

Topics

- * What is Personally Identifiable Information (PII)?
- * Why are we committed to protecting PII?
- * What laws govern us?
- * How do we comply?
- * What is PCI Compliance?
- * How do we protect the University from fraud?

Our Commitment

EMU is committed to protecting the personally identifiable information of its students, faculty, staff, and other individuals associated with the University.

What is PII?

1. Any information about an individual that can be used to distinguish or trace an individual's identity
 - * Social Security Number
 - * Date and Place of Birth
 - * Mother's Maiden Name
 - * Biometric Records
2. Any other information that is linked or linkable to an individual
 - * Medical Information
 - * Education Information
 - * Financial Information

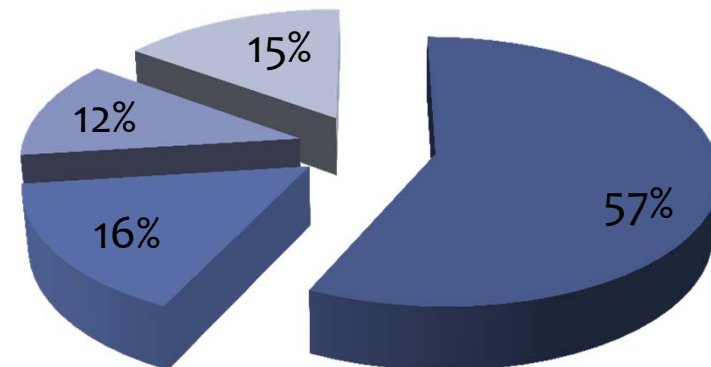
The important thing to remember:
the more information that is
combined the greater the risk of
identifying a specific individual

E.g., A social security number without a name is unlikely to result in the identification of an individual; however, a name and social security number are very likely to result in the identification of an individual

12 Months 2012

- * 1/2012 University of Miami – 1,219 patients notified that flash drive stolen from pathologist’s car
- * 2/2012 University of NC at Charlotte – 350,000 SSN and financial data on internet due to a configuration error
- * 3/2012 Hackensack University Medical Center – employee stole 445 patients names, addresses, DOB, SSN, drivers license numbers, and insurance information
- * 3/2012 Brigham Young University – 1,300 student’s names, email addresses, phone numbers and student ID numbers attached to an email
- * 4/2012 Case Western Reserve University – stolen university laptop containing 600 alumni's name and SSN

Data Loss



Source: <http://datalosddb.org>

What Laws Govern Our University?

- * The Red Flags Rule: Requires the University to develop and implement a written Identity Theft Prevention Program, to detect, prevent and mitigate identity theft in connection with certain financial accounts
 1. Any accounts where Eastern is acting as a creditor
 2. And is primarily for personal, family or household purposes
 3. And involved in multiple transactions
 - * Student Loan Information
 - * Student Payment Plans

What Laws Govern Our University?

- * Gramm–Leach–Bliley Act (GLBA): Requires the University to take steps to ensure the security and confidentiality of customer records
 - * Name
 - * Address
 - * Phone Number
 - * Bank and Credit Card Number
 - * Income and Credit History
 - * Social Security Number

What Laws Govern Our University?

- * Health Insurance Portability and Accountability Act of 1996 (HIPAA): the privacy rule addresses the use and disclosure of individuals' health information—called “protected health information”
 1. Past, present or future physical or mental health conditions
 2. Provision of health care to the individual
 3. Past, present, or future payment for the provision of health care to the individual
- * Common Identifiers:
 - * Name
 - * Address
 - * Birth Date
 - * Social Security Number

What Laws Govern Our University?

- * Family Educational Rights and Privacy Act (FERPA):
Protects the privacy of student education records.
Student educational records may **ONLY** be disclosed to a third party with the consent of the student as specified by the law.
- * See the Office of Records and Registration web page for exceptions:
- * http://www.emich.edu/registrar/registration_info/ferpa.php

Technology Security and PII Protection

- * **Safeguards Rule** – EMU has implemented a University-wide information technology security program to protect customer information called the Information Security Program (ISP)
- * Any unauthorized access (physical, remote or otherwise) to university computer systems as well as malicious attempts to disrupt information technology services is a violation of Eastern Michigan University Policy
- * **All suspected incidents should be reported to the IT Help Desk**

734-487-2120

Best Practice for Technical Security of PII

- * Always ensure that your computer is logged off or password protected when you are not present
- * Do not share your passwords
- * Do not download or store PII on laptops or any portable devices, unless absolutely necessary. Portable devices containing PII should be encrypted.
- * Ensure that shared drives are secure when storing files containing PII.
- * Ensure that all files containing PII are encrypted or utilize SFTP
- * Limit access to sensitive information; need to know only
- * Ensure that all servers are appropriately protected, consult DoIT

Best Practice for Physical Security of PII

- * Only ask for PII when absolutely necessary to conduct the business of the University
 - * If individuals supply supplemental PII that is not needed, destroy (shred) it or redact it immediately; DO NOT KEEP IT
 - * All documents containing PII must be stored in locked cabinets; a locked office alone is not acceptable
 - * All documents containing PII must be destroyed when no longer needed; documents regularly collected must have a record retention schedule

Best Practice for Physical Security of PII

- * Document the handling of PII within relevant procedures
- * If student workers have access to PII, have them sign a confidentiality agreement and be sure to explain the importance of and the responsibility to protect the information
- * Do not email or fax documents containing PII; utilize the postal service or hand delivery
- * As a general rule do not share PII

Disclosure of FERPA Protected Information

- * **Disclosure of information from confidential educational records is limited to the eligible student or to others:**
 1. To whom the eligible student releases the records;
 2. Who have a “Legitimate Educational Interest”
 3. Who are entitled or permitted to know the content of the records by virtue of one or more FERPA “exceptions.”
- * **Items 2 and 3 above are strictly defined under FERPA,** before releasing any information subject to FERPA please consult with:

The Registrar Office 734-487-2382
General Counsel’s Office 734-487-3246

FERPA “Danger Zones” for Faculty and Instructional Staff

- * Circulating a printed class list with student name and Student ID number or grades as an attendance roster
- * Discussing the progress of any student with anyone other than the student without the consent of the student (e.g., parents, employers, other students)
- * Providing anyone with lists of students enrolled in your classes for any commercial purpose
- * Providing anyone with student schedules or assisting anyone other than university employees in finding a student on campus
- * Giving out directory information about a student who has requested confidentiality

FERPA “Danger Zones” for Faculty and Instructional Staff

- * Disclosing confidential information to a third party without authorization
- * Linking the name of a student with that student's ID number in any public manner
- * Including personally identifiable information about student A in student B's record without student A's permission
- * Including FERPA protected information in a letter of reference without the student's written permission (this includes the student's GPA or grade in your class)

FERPA “Danger Zones” for Faculty and Instructional Staff

- * Leaving graded tests in a stack for students to pick up by sorting through the papers of all students. You may leave them with an assistant and/or receptionist to give out to the student and you may place each test in a sealed envelope with the student’s name on it.
- * Requiring students to use social security numbers, student ID numbers, birthdays, phone numbers, auto tag numbers, or derivatives of those numbers. Use a pin number that only the professor and the student know.

To avoid FERPA “Danger Zones” regarding posting grades:

- * NOT Post the grades, even if coded, in alphabetical order or any other recognizable order
- * If you are giving out grades or other FERPA protected information over the phone, make sure that the person you are speaking to is your student. Ask questions that only the student could answer, such as the name of the course, an example of an assignment from the course, or questions that were on the final exam.

What is PCI-DSS Compliance?

- * Payment Card Industry-Data Security Standards
 - * Establish proper handling of credit and debit card transactions processed by any department and/or group affiliated with the University
 - * Ensure cardholder information, such as sensitive account and personal cardholder information, is protected against theft and/or improper usage

Contact Student Business Services

734-487-8481

Compliance by Eastern Michigan University requires:

- * PCI-DSS compliance is mandatory for any department that accepts, captures, stores, transmits and/or processes credit or debit card information
- * Only authorized and properly trained individuals may accept and/or access credit or debit card information
- * Credit and debit card payments may be accepted only using methods approved by the University Student Business Services Office
- * Each person who has access to credit or debit card information is responsible for protecting the information

PII Data Loss Prevention & Reporting

- * What do I do if I observe the improper handling of PII?
 - * Immediately contact the Associate Vice President for Finance, CIO, or Registrar
- * What do I do if I know of a data breach?
 - * Immediately contact the CIO or Legal Counsel
 - * Andrea Jaeckel 734-487-3328
 - * Carl Powell 734-487-1491
 - * Chris Shell 734-487-2382
 - * Gloria Hage 734-487-3246

What is Fraud?

- * Misappropriation of funds, securities, supplies, or other assets
- * Impropriety in the handling or reporting of money or financial transactions
- * False Reporting of Work Time
- * Disclosing confidential and proprietary information to outside parties
- * Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the University. Exception: Gifts, meals and entertainment less than a nominal amount in value
- * Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment

What is Fraud?

- * Forgery or alteration of any document or account belonging to Eastern Michigan University
- * Destruction, alteration, mutilation, concealment, covering up, falsification, or making of a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence any investigation by or on behalf of the University
- * The destruction, alteration, or concealment of any records used in the conduct of an audit

Fraud Prevention

- * What do I do if I suspect fraud?
 - * Immediately contact the Vice President and Secretary to the Board of Regents, General Counsel, or the Chief Financial Officer
 - * Gloria Hage 487-3246
 - * John Lumm 487-2031
 - * Vicki Reaume 487-2410
 - * DPS 487-1222

- * Visit <http://www.emich.edu/regents/> “Anonymous Ethics and Compliance Reporting”

Additional Resources

- * EMU Incident Response Team
<http://it.emich.edu/security/incident/faq.cfm>
- * The Federal Trade Commission (FTC): www.ftc.gov
- * GLBA at the FTC:
www.ftc.gov/privacy/privacyinitiatives/glbact.html

Additional Resources

- * EMU Records and Registration
http://www.emich.edu/registrar/registration_info/ferpa.php
http://www.emich.edu/registrar/registration_info/ferpa_facultystaff.php
- * EMU Authorization to Release FERPA protected information form- <http://www.emich.edu/sbs/docs/consent.pdf>
- * Department of Education
<http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Additional Resources

- * Identity Theft Resource Center: <http://www.idtheftcenter.org/>
- * Federal Trade Commission – Fighting Back Against Identity Theft: <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
- * U.S. Department of Education, Office of the Inspector General - Resource on Identity Theft for Students: <http://www2.ed.gov/about/offices/list/oig/misused/idtheft.html>
- * U.S. Identity Theft Task Force: <http://www.idtheft.gov/>
- * Anonymous Ethics and Compliance Reporting <http://www.emich.edu/regents/>