PII- Personally Identifiable Information-Training
What is PII?

- PII = Personally Identifiable Information
- EMU is committed to protecting the privacy of personally identifiable information of its students, faculty, staff, and other individuals associated with the University.
What is PII?

- Any information about an individual that can be used to distinguish or trace an individual’s identity
  - Social Security Number
  - Date of Birth
  - Mother’s Maiden Name
  - Biometric Records
- 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.

Example: 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.
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
4/12 Case Western Reserve University – stolen university laptop containing 600 alumni's name and SSN
All entities of the University will take appropriate measures, implement necessary technology, and/or establish operating procedures to ensure data privacy is maintained.

The following training will address policies/acts that are essential to the adherence of EMU’s privacy policy, including:

- Red Flag Rules
- PCI Compliance
- Gramm Leach Bliley Act
- FERPA
Red Flag Rules
What are the Red Flag Rules?

- Red Flags Rule is a federal regulation issued by the Federal Trade Commission (FTC) as part of the implementation of the Fair and Accurate Credit Transaction (FACT) Act of 2003. Red Flags Rule requires financial institutions and creditors to implement a written Identity Theft Prevention Program and to provide for the continued administration of this Identity Theft Prevention Program.
To detect Red Flags and stop identity thieves from using someone else’s identifying information to commit fraud.
**Terms & Definitions You Should Know**

- **Covered Accounts**: an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account. Any account that the financial institution or creditor offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

- **Creditor**: any person, corporation, government or government subdivision or agency, trust, estate, partnership, cooperative, or association who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.
Identifying Information - is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including:

- Name
- Address
- Telephone number
- Social security number
- Employer or taxpayer identification number
- Computer Internet Protocol address
- Date of birth
- Government issued driver’s license
- Alien registration number
- Government passport number
- Student identification number
- Routing code

Identity Theft - a fraud committed or attempted using the identifying information of another person without authority

Red Flag - a pattern, practice, or specific activity that indicates the possible existence of identity theft
Why does Red Flags Rules apply to EMU?

- The Red Flags Rule does not name specific types of institutions that must comply. Instead, compliance requirements are based on the types of accounts EMU has with students.
- The Rule is generally based on the existence of covered accounts. Covered accounts include
  - student accounts in which the University does not require full tuition payment at the time of enrollment
  - professional service providers (clinics) that bill after service is delivered
  - student loans administered by the University (i.e. Federal Perkins Loans).
Under the Red Flags Rule, EMU is required to establish a written "Identity Theft Prevention Program". The plan includes procedures to detect, prevent, and respond to patterns, practices, or specific activities that may indicate identity theft.

The program is approved by EMU Board of Regents and is updated and monitored according to changes in risk. The University Privacy Work Group is responsible for the oversight, training of staff, and audit compliance to accomplish the following:

- **Identify Red Flags** for new and existing covered accounts and incorporate those Red Flags into the Program
- **Detect Red Flags** that have been incorporated into the Program
- **Respond to Red Flags** identified in the Program appropriately to prevent and mitigate identity theft.
- **Ensure the program is updated** periodically to reflect changes in risks to students and customers.
1. Notification and Warnings from Credit Reporting Agencies

- **Red Flags**
  - Report of fraud accompanying a credit report
  - Notice or report from a credit agency of a credit freeze on an applicant
  - Notice or report from a credit agency of an active duty alert for an applicant
  - Receipt of a notice of address discrepancy in response to a credit report request
  - Indication from a credit report of activity that is inconsistent with an applicant’s usual pattern or activity
Identification of Red Flags

2. Suspicious Documents
   ▪ Red Flags
     ▪ Identification document or card that appears to be forged, altered or inauthentic
     ▪ Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document
     ▪ Other document with information that is not consistent with existing student information
     ▪ Application for services that appears to have been altered or forged
3. Suspicious Personal Identifying Information

- Red Flags
  - Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates)
  - Identifying information presented that is inconsistent with other sources of information (example: an address not matching an address on a loan application)
  - Identifying information presented that is the same as information shown on other applications that were found to be fraudulent
4. Suspicious Covered Account Activity or Unusual Use of Account

- **Red Flags**
  - Change of address for an account followed by a request to change the student’s name
  - Payments stop on an otherwise consistently up-to-date account
  - Account used in a way that is not consistent with prior use
  - Mail sent to the student is repeatedly returned as undeliverable
  - Notice to the University that a student is not receiving mail sent by the University
  - Notice to the University’s that an account has unauthorized activity
  - Breach in the University’s computer system security
  - Unauthorized access to or use of student account information
5. Alerts from Others
   - Red Flag
     - Notice to EMU from a student, identity theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in identity theft
Detecting Red Flags

Student Enrollment
- To detect any of the Red Flags identified above associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the person opening the account
- Require certain identifying information such as name, date of birth, academic records, home address or other identification
- Verify the student’s identity at time of issuance of student identification card (review driver’s license or other government-issued photo identification)

Existing Accounts
- To detect any of the Red Flags identified about for an existing covered account, University personnel will take the following steps to monitor transactions on accounts
- Verify the identification of students if they request information (in person, via telephone, facsimile or email)
- Verify the validity of requests to change billing address by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes
- Verify changes in banking information given for billing and payment purposes

Consumer (“Credit”) Report Requests
- To detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, University personnel will take the following steps to assist in identifying address discrepancies
- Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report was made to consumer reporting agency
- In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate
Respond to Red Flags

Preventing and Mitigating Identity Theft
- In the event that University personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:
  - Continue to monitor a covered account for evidence of identity theft
  - Contact the student or applicant for which the credit report was requested
  - Change any passwords or other security devices that permit access to covered accounts
  - Do not open a new covered account
  - Provide the student with a new student identification number
  - Notify the Program Administrators for determination of the appropriate step(s) to take
  - Notify law enforcement
  - Determine that no response is warranted under the particular circumstances

Protecting Student Identifying Information
- To further prevent the likelihood of identity theft occurring with respect to covered accounts, the University will take the following steps as they relate to internal operating procedures:
  - Ensure that the EMU website is secure or provide clear notice that the website is not secure
  - Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information
  - Ensure that office computers with access to covered account information are password protected
  - Avoid use of social security numbers
  - Ensure computer virus protection is up to date
  - Require and keep only the kinds of student information that are necessary for University purposes
The Committee will periodically review and update this Program to reflect changes in risks to students and soundness of the University from identity theft. In doing so, the Committee will consider the University’s experience with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the University’s business arrangements with other entities. After considering these factors, the Program Administrators will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.
Credit Card Processing and Security Policy
What is the purpose of the policy?

- 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.
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.

- Credit and Debit card payments may only be accepted in the following manner:
  - In person
  - Via Telephone
  - Via Fax
  - Via Physical Mail (not e-mail), with special approval
Compliance by Eastern Michigan University Requires:

- Each person who has access to credit or debit card information is responsible for protecting the information.

- The following pieces of information are considered “confidential” and must be protected from initial capture through destruction regardless of the storage mechanism used:
  - Credit or debit card number and expiration date
  - Cardholder Verification Value (CVV2)
  - Personal Identification Number (PIN)
  - Cardholder’s name, address and/or phone number when used in combination with the above fields

- Credit and debit card information must be destroyed as soon as it is no longer necessary.
  - Physical documents, such as customer receipts, merchant duplicate receipts, reports, etc., that contain credit or debit card information should be retained only as long as there is a valid business reason to do so, and no longer than 90 days.
  - While the documents are retained, they must be stored in locked cabinets in a secured area with restricted access to authorized individuals on a need-to-know basis.
Credit and debit card information must be destroyed as soon as it is no longer necessary.

Physical documents, such as customer receipts, merchant duplicate receipts, reports, etc., that contain credit or debit card information should be retained only as long as there is a valid business reason to do so, and no longer than 90 days.

While the documents are retained, they must be stored in locked cabinets in a secured area with restricted access to authorized individuals on a need-to-know basis.
Compliance by Eastern Michigan University Requires:

- Departments must maintain checks and balances in the handling of credit and debit card information.
  - All departments and offices must settle credit card terminals daily and report credit card revenue within 2 business days to the University Student Business Services Office via Cash Deposit Voucher.

- Each department that handles credit and/or debit card information must have documented procedures for complying with this policy and PCI-DSS.
Compliance by Eastern Michigan University Requires:

- Department and office procedures must include, but are not limited to the following:
  - Segregation of duties
  - Deposits
  - Reconciliation procedures
  - Physical security
  - Disposal
  - Cash register procedures (if applicable)

- Suspected theft of credit or debit card information must be reported to the University Student Business Services Office and University Department of Public Safety.
Gramm Leach Bliley Act
What is GLBA?

- **Gramm Leach Bliley Act**
  - A Federal law requiring all financial institutions to develop, implement, and maintain safeguards to protect customer information
  - Comprised of several parts, most notably the Privacy Rule (16 CFR 313) and the Safeguards Rule (16 CFR 314)
Privacy Rule- each institution has an obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.

Safeguards Rule- requires all financial institutions to develop an information security program, which is defined as: administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.
Customer Information- any record containing non-public personal information about a customer of a financial institution- can be paper, electronic, or other form

Non-public personal information- personally identifiable financial information that is provided by a consumer to a financial institution. Examples include:
- Social Security Number
- Date of Birth
- Financial Account Numbers or Credit Card Numbers
- Name, Address, and Phone Numbers (when collected with financial data)
- Details of any financial transaction
EMU significantly engages in providing student loans and other financial services and as such, falls within the definition of a Financial Institution under GLBA and must comply:

- Examples of financial information regulated by GLBA include:
  - Student or other loans
  - Collection of delinquent loans
  - Check cashing services
  - Financial or investment advisory services
  - Obtaining information from a consumer report
  - Career counseling services for those seeking employment in finance, accounting or auditing
Privacy Rule- The FTC has stated that any college or university that complies with FERPA and that is also a financial institution subject to the requirements of GLBA shall be deemed to be in compliance with GLBA’s privacy rules if it is in compliance with FERPA.
How Does EMU Comply?

- **Safeguards Rule**: EMU has implemented a University-wide information technology security program to protect customer information called the Information Security Program (ISP)
Coordination of the ISP

- Shared between the Chief Information Officer (CIO) and the University’s Registrar

- Adherence to the University’s ISP and the requirements of the GLBA is the responsibility of supervisors and employees in departments that access data which is governed or regulated

- Operational areas across the University are responsible for implementing a unit-level security plan
Implementation of the information security program is the shared responsibility of Information Technology, Records and Registration, Financial Aid, Student Business Services, Human Resources, and Payroll. Each unit is responsible for implementing programs to safeguard sensitive and protected data and to secure student information.

**Example: IT Risk Mitigation Systems:** IT maintains policies, procedures, and processes that protect against anticipated threats to the security or integrity of electronic students information and guard against unauthorized use of such information. This includes:

- Data access authorization policies
- Network firewalls, intrusion detection systems and intrusion prevention systems
- Digital forensic and security analysis programs
Training and Education

- All University employees will be instructed in the importance of confidentiality of customer information before access to such is granted. Included in the instructions are the privacy requirements under:
  - Family Educational Rights and Privacy Act (FERPA)
  - Health Insurance Probability and Accountability Act (HIPAA)
  - Safeguard Requirements of GLBA
  - Michigan Freedom of Information Act (FOIA) exemptions
The University has established a policy for central reporting and tracking of serious incidents. The Incident Response Team (IRT) is responsible for handling information system security incidents.
EMU takes reasonable steps to select and retain service providers who maintain appropriate safeguards. The evaluation for choosing a service provider and contracts for service must meet strict provisions for securing confidential information.
FERPA
Family Educational Rights and Privacy Act
What is FERPA?

- The Family Educational Rights and Privacy act of 1974 is a federal law designed to protect the privacy of current and former student's educational records and afford students certain rights with respect to their education records.
What are a student’s rights under FERPA?

- The right to inspect and review the student's education records within 45 days of the day EMU receives a request for access.
- The right to request the amendment of the student's education records that the student believes are inaccurate or misleading.
- The right to file a complaint with the U.S. Department of Education concerning alleged failures by EMU to comply with the requirements of FERPA.
- The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent.
EMU has designated the following items as directory information and these items may be included in publications or disclosed upon request without consent:

- Name
- Address
- Email Address
- Telephone Listing
- Date and Place of Birth
- Enrollment Status
- Major field of study
- Participation in recognized activities and sports
- Weight and height of members of athletic teams
- Dates of attendance
- Degrees and awards received (including, but not limited to, the Dean's List)
- Most recent previous educational agency or institution attended by the student.

EMU reserves the right to make directory information public unless a student's written objection (specifying the category of information not to be made public without prior consent) is filed at the Office of Records and Registration within 14 days after each term begins.
Disclosure of information from confidential educational records is limited to the eligible student or to others:

- To whom the eligible student releases the records
- Who have a “Legitimate Educational Interest”
- Who are entitled or permitted to know the content of the records by virtue of one or more FERPA “exceptions”
Examples of FERPA Protected Information

- Grades
- Test Scores
- I.D. Numbers or Social Security Numbers
- Financial Records
- Disciplinary Records
- Class Schedule
Example of records NOT education records under FERPA

- Sole Possession Records
- Law Enforcement Unit Records
- Employment Records
- Medical Records
- Post-Attendance Records
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 basis 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 deliver
- As a general rule, do not share PII
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
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
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
EMU Records and Registration:
http://www.emich.edu/registrar/registration_info/ferpa.php

EMU Authorization to Release FERPA protected information form:
http://www.emich.edu/sbs/docs/consent.pdf

Department of Education
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/

  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/