DATA SECURITY

PRESENTED BY WILL MESSIER | FEBRUARY 2017

REVIEW

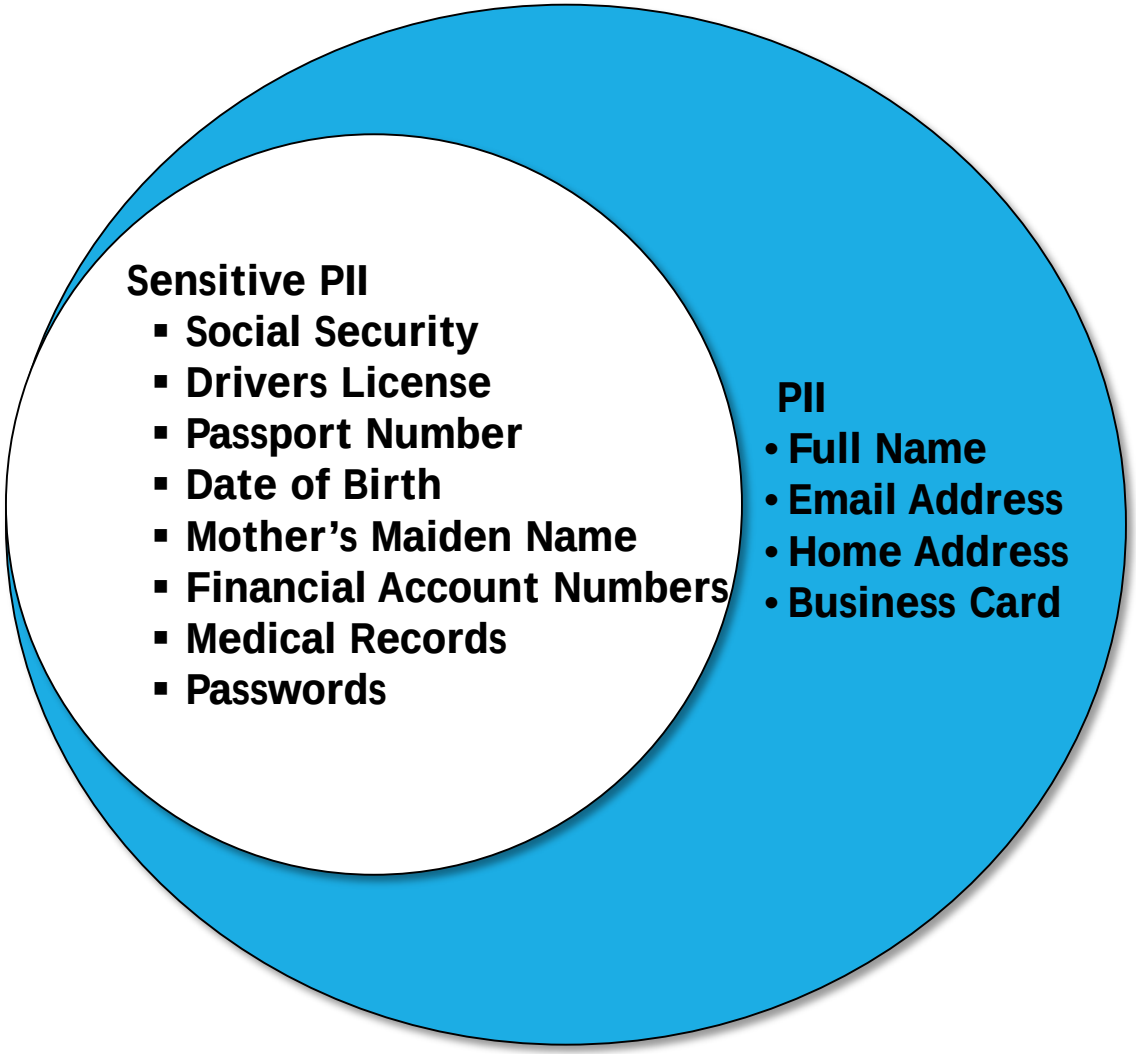
WHAT IS PERSONALLY IDENTIFIABLE INFORMATION?

Personally Identifiable Information (PII)

- Any information about an individual maintained by an organization, including
- Any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

As an MEP employee or contractor, you are responsible for protecting this data

Examples of PII

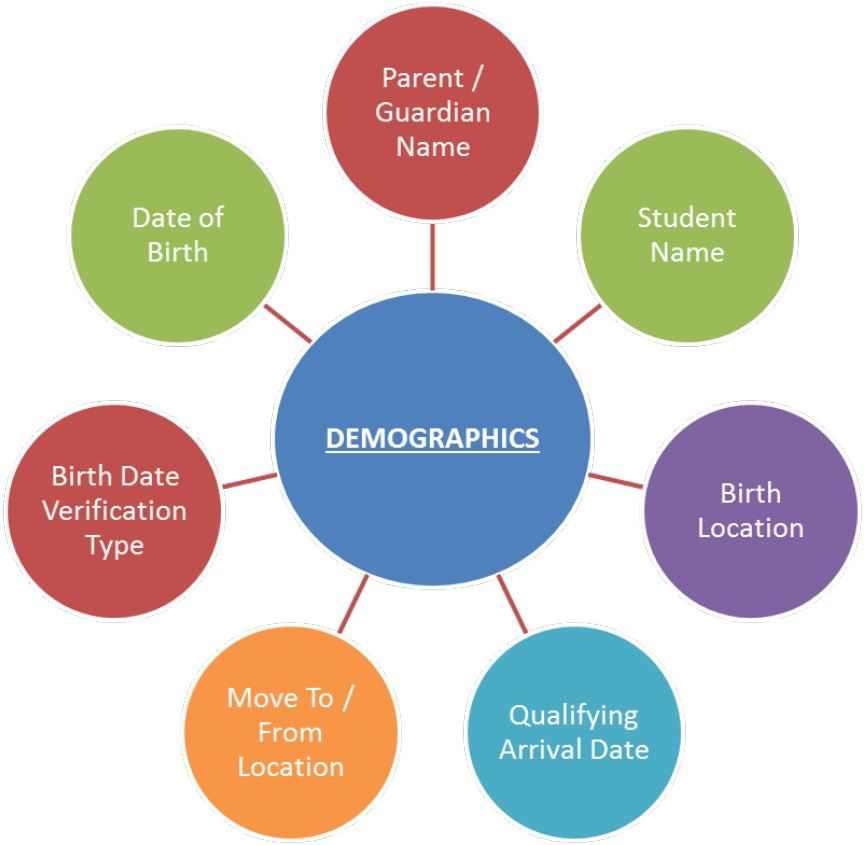


Combining pieces of non-sensitive information could result in a set of information that is sensitive

E.g. Answer to security questions

Migrant Student Data

- Migrant student information collected through the Certificate of Eligibility (COE) includes Sensitive PII
- Collection, transmission, and storage of this information must be protected
- Only access the necessary data to perform your job duties (e.g. official purposes related to providing services)



Family Educational Rights and Privacy Act (FERPA)

- Protects the disclosure of PII and educational records of students
- Governs who has access to this data

FERPA Exceptions

- School officials with legitimate educational interest
- Other schools to which a student is transferring
- Specified officials for audit or evaluation purposes
- Appropriate parties in connection with financial aid to a student
- Organizations conducting certain studies for, or on behalf of, the school
- Accrediting organizations
- To comply with a judicial order or lawfully issued subpoena
- Appropriate officials in cases of health and safety emergencies
- State and local authorities within a juvenile justice system pursuant to specific state law

POLICY

BEHAVIOR | DEVICES | COMMUNICATION

Rules of Behavior

- Ensure only authorized employees have access to private information
- Keep documents containing PII in a locked container
- Ensure Migrant Education Program information is not released without consent
- **Never** share your account passwords with anyone else. You are responsible for all actions taken with your credentials
- Staff should create $TR0ng passwords that use a combination of uppercase letters, lowercase letters, numbers, and symbols, and are changed regularly

Rules of Behavior

- Log off computers whenever they are not in use
- Be aware of individuals around you who can see your keyboard as you type in passwords
- Be aware of social engineering and scams. These include phony calls from help desks claiming to offer support for a problem you were not aware of, or suspicious emails asking you to click a link and enter your credentials

Device Security

- All devices containing PII should be encrypted and use a strong password to gain access
- Mobile devices accessing PII should have a PIN
- Make sure antivirus is always up-to-date
- When transporting a device in a car, place it in the trunk. Never leave it in a car for a long period of time or overnight
- Do not leave devices out in a hotel room, and store devices in a safe if possible
- At the airport, never place devices in checked luggage

Secure Communications

- TRANSMISSION OF PERSONALLY IDENTIFIABLE INFORMATION OVER THE INTERNET MUST ALWAYS BE ENCRYPTED!
- Email accounts should use two-factor authentication
- PII cannot be placed in the body of an email; instead, it must be sent as an encrypted attachment
- The password for an encrypted attachment must be sent through a different form of communication
  - Phone call
  - Text
  - Previously known password

QUESTION

"Can I just send the password in a second email?"

NO

BREACH OF DATA

RISKS | CAUSES | REPORTING

Risks of improper handling

Risks to ***Migrant Children and Families***

- Identity theft, financial loss, and/or credit damage
- Emotional distress
- Loss of confidence in the government

Risks to ***MEP Employees***

- Disciplinary action resulting in: loss of clearance, loss of access to PII, or loss of employment
- Penalties under the Family Educational Rights and Privacy Act
- Diminished reputation

Risks to the ***MEP***

- Diminished reputation
- Costs of mitigation and/or litigation
- Impact on agency processes
- Loss of the public trust

Causes

- Can be a simple mistake, such as sending an email with PII to the wrong recipient
- Can be the result of a computer virus infection
- Can be theft of device
- Lack of use of encryption
- Many more

- Better safe than sorry- report any warning signs

Reporting

- Step 1: Contain the breach
- Step 2: Contact immediate supervisor
- Step 3: Document the breach

- On occasion, the program director might request that you participate in a detailed evaluation of the events leading to the breach for official records, prevention, and other uses