New Technology, New Challenges

Safeguarding migrant data in the digital era

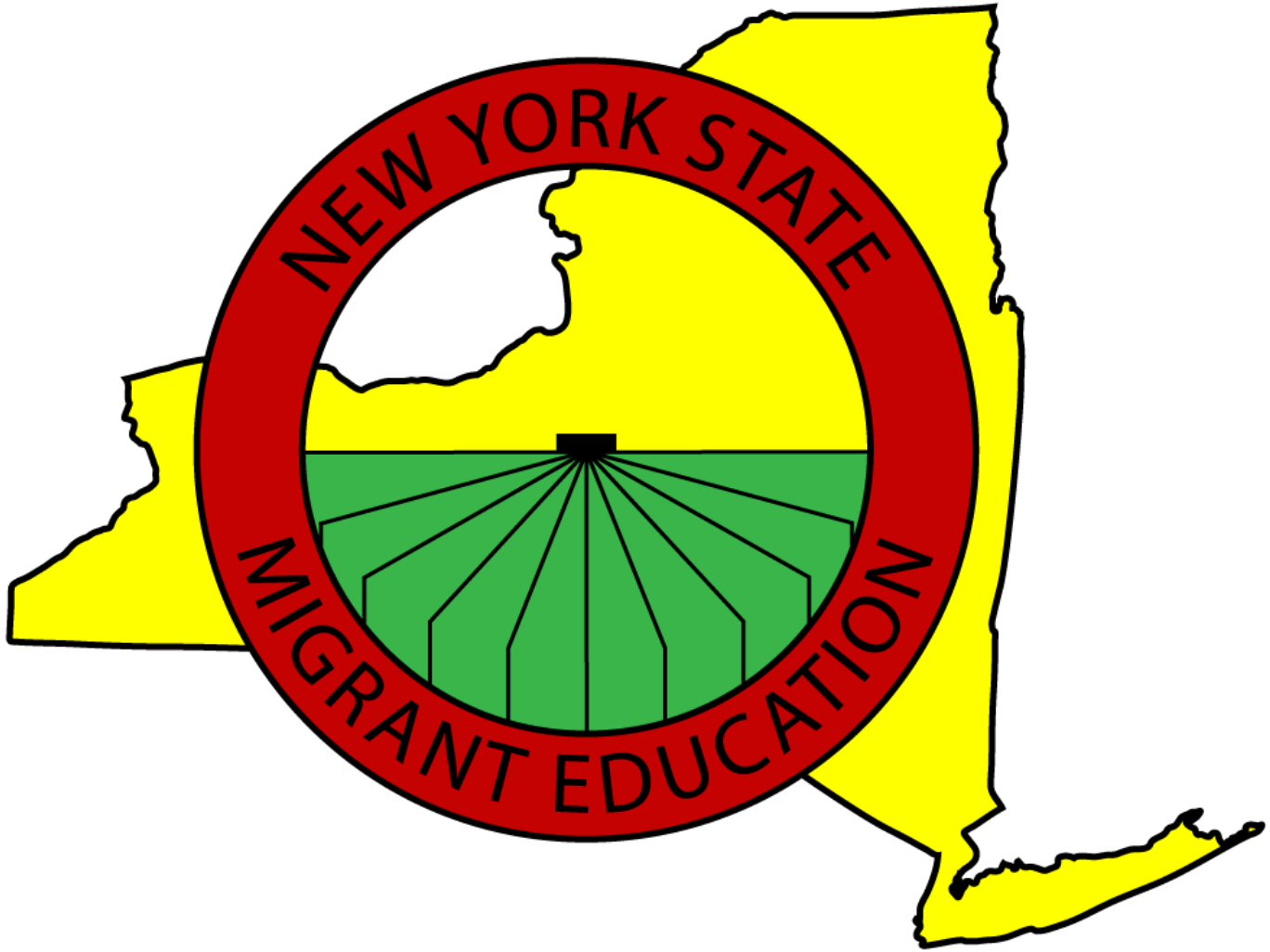
NEW YORK STATE
MIGRANT EDUCATION PROGRAM

About the Presenters

- **Will Messier**
- Director ID/R-MIS2000-MSIX
- Email: wmessier@nysmigrant.org
- (202) 260-1394

- **Robert Hillman**
- Information Systems Assistant
- Email: rhillman@nysmigrant.org

- **Odilia Coffta**
- Data Training Coordinator
- Email: ocoffta@nysmigrant.org



Objectives

Participants will:

- Be familiarized with the concept of cybersecurity and the impact of cyber-attacks
- Be able to identify PII and understand the risks and responsibilities associated with handling it
- Learn about the impact and consequences of improper disclosure of information and inadequate protection of computer resources
- Learn about what steps they can take to protect themselves online
- Learn methods to secure migrant family data in the workplace

Group discussion

- How has technology has made the job of the Migrant Education Program easier?
- How has this made the Migrant Education Program data vulnerable?

Cybersecurity and Cyber Attacks

NEW YORK STATE
MIGRANT EDUCATION PROGRAM

What is Cybersecurity?

- Cyberspace – global online environment of computers and computer communications, including the public internet and private computer networks

- Cyber-attack – disrupting, disabling, destroying, or maliciously controlling a computing environment; or destroying the integrity of the data or stealing controlled information

- Cybersecurity – ability to protect or defend the use of cyberspace from cyber attacks

Who are the Victims of Cyber-Attacks?

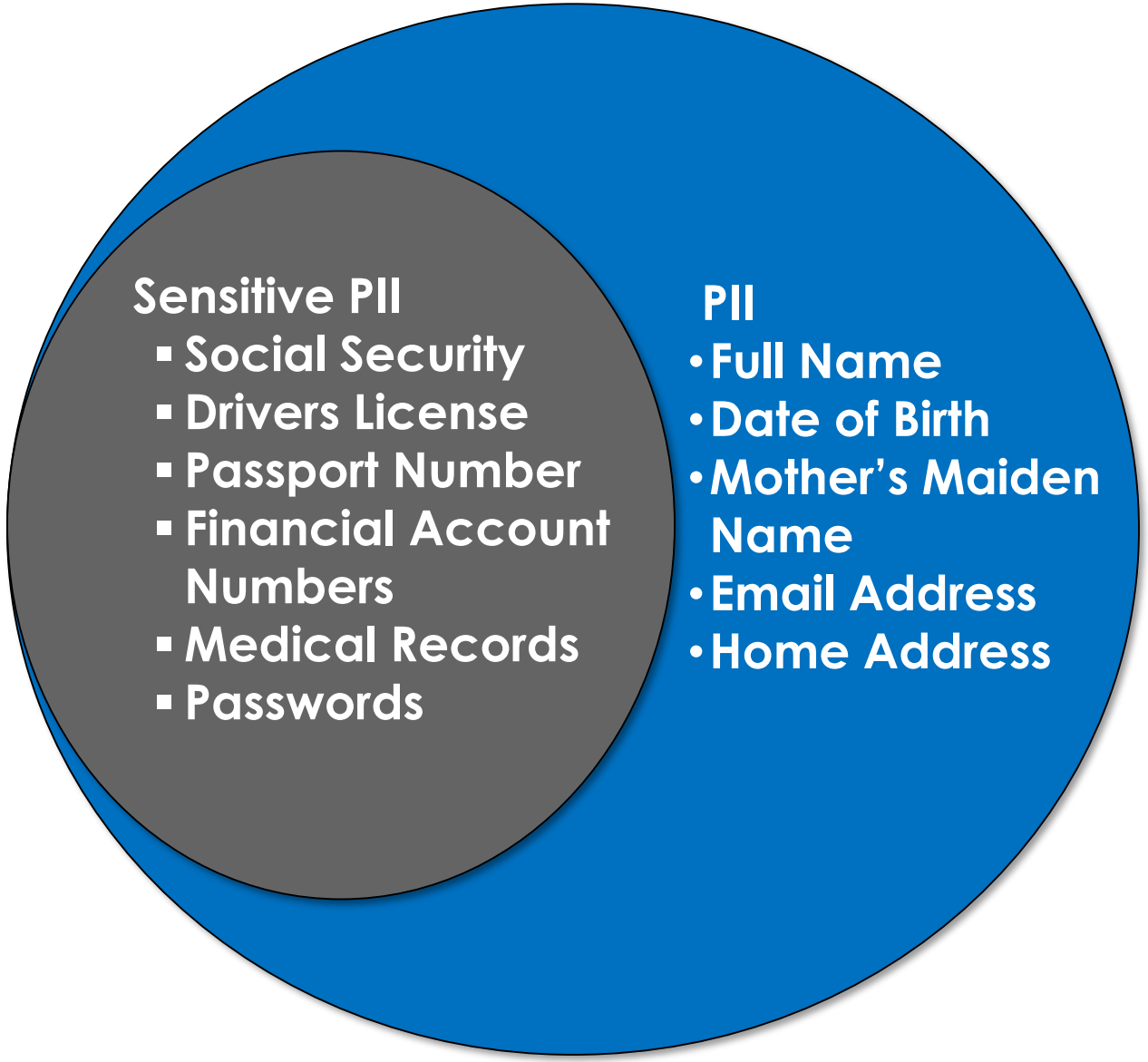
Personally Identifiable Information

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

Examples of PII and SPII

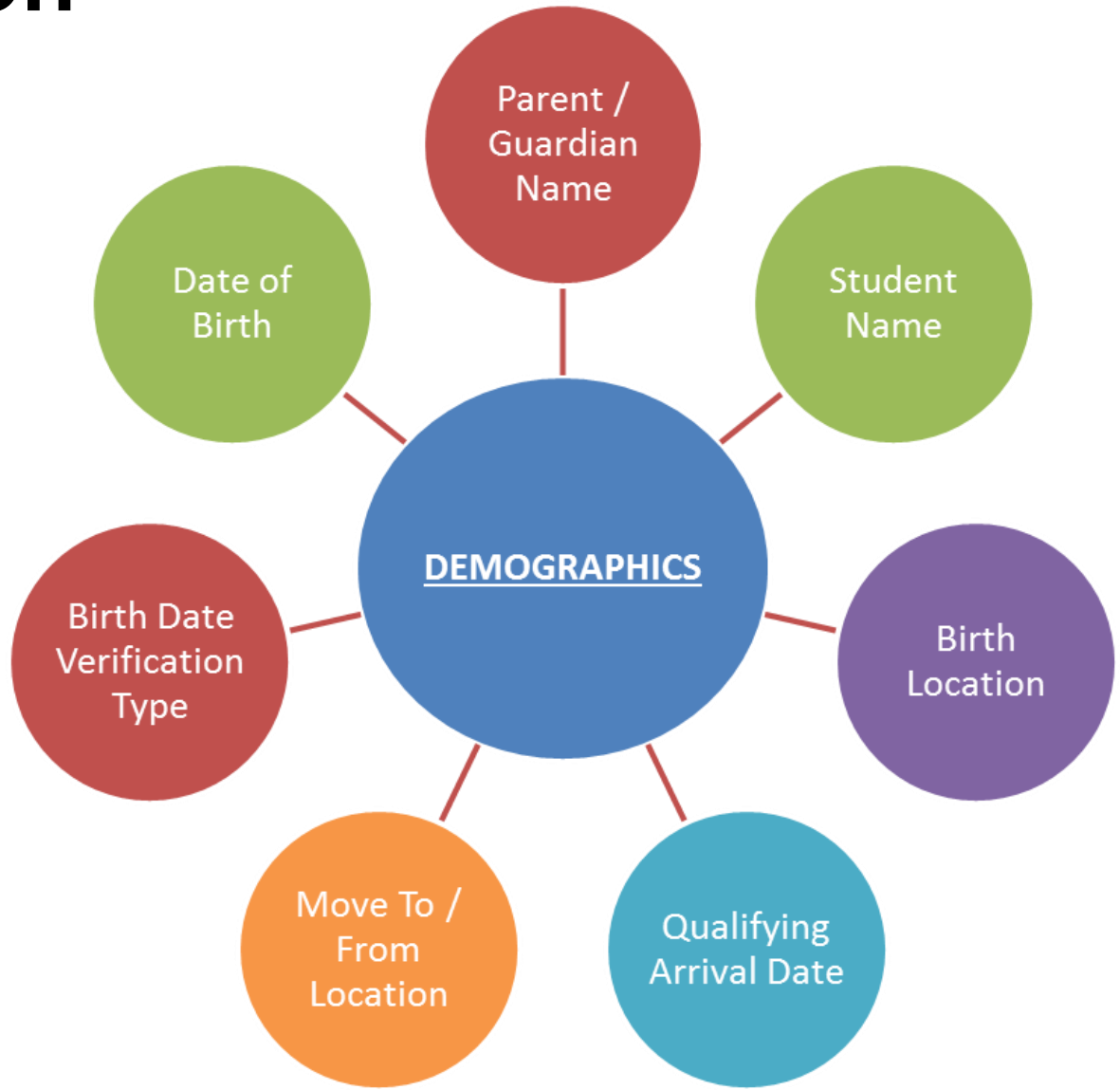


Combining pieces of non-sensitive information could result in a set of information that is sensitive

E.g. Answer to security questions

Migrant Student Information

- 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 (34 CFR § 99.31)

- 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

Developing a security policy

Data Security Checklist

- Verify if your governing institution already has a data security policy already in place
- Create process to follow in the event of a data breach
- Secure devices and methods of communication
- Train your staff on data security procedures

The three-pronged approach

Train users

Encrypt devices

Secure communications

Example User Security Policy Elements

- Rules for User Data Access:
  - Ensure only authorized employees have access to private information
  - Follow the Principle of Least Privilege. Give employees access only to the minimum amount of PII needed for them to perform their jobs.
  - Ensure Migrant Education Program information is not released without consent in accordance with FERPA.
- User Credentials or Passwords:
  - Never share your account passwords or passphrases with anyone else. You are responsible for all actions taken with your credentials
  - Staff should create STRONG passwords or passphrases that use a combination of uppercase letters, lowercase letters, numbers, and symbols, and are changed at least twice a year

Example Data Security Policy Elements

- Data Protection:
  - Physical documents containing PII should be kept in an area accessible only to staff and that can be locked during non-business hours
  - Unattended computers should be locked (e.g. using the keystroke [Windows] + [L]) or logged off
  - Proper destruction methods should be observed when disposing of physical or electronic media
    - Simply deleting files from your computer does not erase them completely, and they can often still be recovered with special software. Be sure to follow appropriate procedures for the type of media to ensure that the data is completely erased!

What is a data breach?

- PII that is **lost, stolen, disclosed, or otherwise exposed to unauthorized people and/or for unauthorized purposes**
- May be caused by improper use of:
  - **Storage Media** – Saving COEs or other documents with student data on unencrypted hard drives or on removable media without encryption
  - **Communications** – Sending sensitive information, combination of non-sensitive information or documents without encryption
  - **Networking** – Reviewing student records in public areas or using public Wi-Fi without a secured connection

Immediately report a suspected or confirmed data breach as soon as it is noticed. It is important that the reporting procedure is made known to everyone and is easy to follow.

Risks of Improper PII Handling **and Breaches**

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 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

Secure Devices

Securing your Devices:

- All computers containing PII should be encrypted
- Have an up-to-date antivirus
- Use a PIN or fingerprint to secure mobile devices
- Accounts with access to PII should use a strong password or passphrase AND two-factor authentication whenever possible

When transporting your laptop or mobile device:

- If you must leave it in a car, lock it in the trunk
- Do not leave it in a car overnight
- Avoid leaving it exposed in a hotel room, or lock it inside an in-room safe if possible
- When flying, never place it in checked luggage.

Secure Transfer & Communication

Protecting PII in Communications

- Email the PII within an encrypted attachment with the password provided separately (e.g., phone call, text, previously known password, or in person)
- Refer to your state policies and procedures for the authorized encryption mechanism
- If available, use a Virtual Private Network (VPN) to encrypt your connection to the internet
- Common file encryption programs include:
  - Microsoft Office – Encrypt Office files
  - Adobe Acrobat Pro – Encrypt PDF files
  - 7zip – Compress & encrypt files

Shoulder Surfing & Social Engineering

- 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

Shoulder Surfing & Social Engineering Cont.

- Emails:
  - Attachments should be scanned with antivirus software, and suspicious attachments should not be downloaded
  - PII should NEVER be put in the body of an email, and should instead be sent as an encrypted attachment using appropriate encryption software
  - Passwords to encrypted documents should be sent through alternative means outside of the email
  - Include a confidentiality notice at the bottom of emails containing such attachments or information

Example confidentiality notice

"This electronic message is intended to be for the use only of the named recipient, and may contain information from the [organization] that is confidential or privileged, or protected FERPA. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of the contents of this message is strictly prohibited. If you have received this message in error or are not the named recipient, please notify us immediately, either by contacting the sender at the electronic mail address noted above or calling the [organization] at [phone number], and delete and destroy all copies of this message."

Finally…

- Always, always check with your governing institutions
- Be patient
- Be proactive
- Understand that this is a constantly changing field

Example Scenario

You received a phone call from a new employee of the Oak Orchard Health Clinic requesting information regarding students residing in Chazy CSD. Amanda, the new employee, would like to know the new address and the children's names of a migrant family that might qualify for services from her program. While you do not know this new person, you and the regional METS have collaborated with the organization for years. You know that they provide important services to migrant children and the parents already gave authorization to share information with this agency based on the Signature section of the COE. **What do you do?**

Frequently asked questions:

- "Can't I just send the password to an attached file in a second email?"
- "How can I refer to the student in an email?"
- "What do I do if a teacher sends me an email about a migrant student containing PII information?"