The Secret Life of PII

Properly Handling Personally Identifiable Information
Objectives

- Recognizing PII
- Understanding TEGL 39-11
- Staff Roles and Responsibilities
- PII Protection and Best Practices
Personally Identifiable Information

Information that can be used to distinguish or trace an individual’s identity.
2 Types of PII

1. Protected PII
   If disclosed, could result in harm to the individual linked to that information.

   **Examples:**
   
   - Social Security Numbers
   - Bank Account Numbers
   - Fingerprints
   - Credit Card Numbers
   - Marital Status
   - Computer Passwords
2 Types of PII

2. Non-sensitive PII

Information that, if disclosed by itself, could not reasonably be expected to result in personal harm.

Examples:

- First and Last Names
- Business Addresses
- Race
- Email Addresses
- Gender
- General Ed. Credentials
Non-Sensitive PII

When combined, could potentially be categorized as protected or sensitive PII.

First and/or Last Name

- Social Security Number
- Date of Birth
- Mother’s Maiden Name
Securing PII

**Hard Copy**
- Locked filing cabinets
- Locked desk drawer
- Properly destroy PII after use

**Electronic**
- Encrypt all emails w/ PII
- **NEVER** email full SSNs
- **NEVER** save PII on unsecured thumb-drives, CDs, etc.
- **Always** lock your desktop!
Encryption Methods (Outlook)

Encrypt & Send

Results for "Encrypt"

Encrypt email messages

Encrypting an email message in Outlook means it's converted from readable plain text into scrambled cipher text. Only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message for reading.

Get a digital ID

On the E-mail Security tab, under Digital IDs (Certificates), click Get a Digital ID. ... You can now send encrypted email in the Microsoft Office Outlook...
Advising Staff About PII

Staff must know:
- The sensitive nature of PII
- Required safeguards to protect PII
- The civil and criminal sanctions for noncompliance

NOTE: PII must only be accessed by those that need the information to perform their job duties.
Best Practices

• Have participants sign releases acknowledging use of PII
• When possible, utilize unique participant identifiers (not SSNs)
• Do not leave records open or unattended
• Immediately report breaches to management
• Use appropriate methods of destroying PII
  • Shredding
  • Securely deleting
What if PII is compromised?

May result in:
- Termination or suspension of funding
- Disciplinary Action

*If PII is compromised, contact your local area’s legal counsel AND notify U.S. Department of Labor
Thank You!

For questions, please contact:

WIOAQNA@jfs.ohio.gov