Properly Safeguarding Personally Identifiable Information (PII)

Ticket Program Manager (TPM)

Social Security's Ticket to Work Program

Goals and Objectives

- Define Personally Identifiable Information (PII)
- Recognize the responsibility of access to PII
- Discover best practices to deter PII violations
- Illustrate how to identify PII loss
- Demonstrate procedures to report a PII loss
- Employ proper communication procedures while working with PII

Message from the Chief Information Officer

- Provides security guidance for SSA employees, contractors, DSS employees and government partners who handle SSA information
- Reminder to properly safeguard personally identifiable information from loss, theft or inadvertent disclosure and to immediately notify management of any PII loss.
- PII includes: person's name, date of birth SSN, bank account information, address, health records and Social Security benefit payment data.

Improper Safeguards

Non-Secure areas in your environment include:

- An office where the public visits
- Public spaces
- An unlocked room
- An unattended desk
- Computers without password protection
- Storage devices (flash drives, CD, etc) that others have access to (non-password protected)

Examples of non secure spaces

- Public space
- Unlocked car
- One one’s desk
- Public locations
- A computer with no password protection
- A flash drive
- A compact disc
- Unlocked room
- An unattended desk

Best Practices

Every individual from users to managers of SSA's automated systems are required to follow agency rules for using SSA systems.

Best Practices to Deter PII violations

- Be familiar with current information on security, privacy and confidentiality practices
- Obtain written authorization before using sensitive or critical applications.
- Use only systems and data for which they have authorization.
- Lock or logoff their workstation/terminal prior to leaving it unattended.
- Act in an ethical, informed and trustworthy manner.
- Protect sensitive electronic records
- Be alert to threats and vulnerabilities to their systems

Responsibility of Managers

- Monitor the use of mainframes, PCs, LANs, and networked facilities to ensure compliance with national and local policies
- Ensure that employee screening for sensitive positions within their components has occurred prior to any individual being authorized access to sensitive or critical applications.
- Implement, maintain and enforce systems security standards and procedures

Responsibility of Managers Continued

- Explain to employees that they are responsible for protecting personal information at all times, both on and off duty.
- Permit employees to access PII only when they need to do their jobs and to disclose it only when appropriate
- Train employees to handle PII responsibly and remind them periodically of their responsibilities to protect all PII they use to complete their work
- When taking records or laptops offsite, lock them in the car's trunk. Do not leave them in the passenger compartment.

Management of Technology

- Do NOT send personal information via email unless it is encrypted. This includes using any PII in the email subject or body.
- Send reports and documents containing PII via regular mail or send them to a secure FAX location.
- Use password protection and encryption software to protect confidential files from unauthorized access.

Management of Technology Continued

- Choose a password that others cannot guess and change it frequently.
- Protect with encryption those peripheral data storage devices such as CDs and flash drives with records containing PII.
- Encrypt files with PII before deleting them from your computer or peripheral storage device. This will ensure that unauthorized users cannot recover the files.
- Lock or log off the computer when leaving it unattended.

Identifying PII Loss

How to Identify PII Loss in Communications

- An unencrypted email sent with a beneficiary's name, SSN, address, phone number or initials.
- Receiving a request via email with a beneficiary’s name, SSN, address, phone number or the initials of a beneficiary.

How to Identify PII Loss in the Work Area

- A co-worker left out a document with personal information on an unattended desk.
- A co-worker moved from their computer that is displaying PII without turning off the monitor or removing the material from the screen.
- Leaving a document with PII unattended at a printer.

Reporting a PII Loss

- Notify a supervisor/manager in your chain of command.
- Manager will complete the “SSA Personally Identifiable Information violation form”.
- Manager will email the completed form to the Quality Assurance Coordinator at TPM.
- TPM will then report to SSA.

Proper Communication with PII

- Through the Ticket Portal
- Fax the Ticket Program Manager: 703.893.4020
- Telephone call
- Encrypted email
- U.S. mail

Questions?

Contact: Lisa Whitaker, Quality Assurance Coordinator

Phone: 703.336.8075

Email: LisaMWhitaker@maximus.com