ACF Security and Privacy Tips

What is PII?

Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity. A solitary piece of information, such as a person's name, qualifies as PII. PII can also be a combination of information, such as a person's name and date of birth.

Additional examples include a photograph, financial account information, biometrics (fingerprints, retina scan, height and weight).

What to do if you think a privacy incident has occurred:

1. ***Report it!*** Contact the ACF Incident Response Team (acf_irt@acf.hhs.gov) AND your supervisor.
2. ***Record it!*** Document where and when the potential incident was found and provide specific details if possible (e.g. URL or subject line).
3. ***Cooperate!*** Promptly respond to inquiries from the ACF Incident Response Team to facilitate a resolution.

Encryption is Key

How to send an encrypted email in Outlook:

- Insert your PIV card into laptop
- Compose a new email (or click the reply or forward button on an existing email)
- Under the Options tab in the new message, select "Encrypt"
- Type your message and click "Send"

Creating Strong Passwords

DOs

- Use at least 12 characters
- Use unique passwords mixing symbols, numbers, and uppercase and lowercase letters

DON'Ts

- DO NOT write down your password
- DO NOT share your password
- DO NOT use words from the dictionary

Try the pass phrase method!

- Choose a phrase that is easy to remember
- Use only the first letter in each word of the phrase
- Substitute numbers for letters wherever possible, e.g. use "2" instead of "to" or "too"
- Include symbols such as "!" or "$"

Example:

The passphrase method is the best way to make a password!

"Tpmitbw2m@p!"

If you collect it, PROTECT IT!

Physically secure documents and devices containing PII by locking them in a cabinet.

Remember to lock your computer screen before walking away by pressing the ⊞+L key.

Only print, extract, or copy sensitive PII when the risk is justified by an official need that is not easily met using other means.

Try to limit the use of PII in email by referencing a ticket number or record ID so the recipient can use it to look up the details themselves.

Encrypt all emails that include PII.

Clean Desk = Safe Desk!

Talk with others using discretion when discussing PII. Consider going to a huddle room.

156 Million

Phishing emails are sent daily

Learn to protect yourself!

PHISHING RED FLAGS

- **FROM:** Is the email from an unexpected source?
- **TIME:** Was the email sent at an unusual time?
- **SUBJECT:** Does the subject match the content?
- **HYPERLINK:** Hover your cursor over a link to check if it points to the expected destination, not a site containing malware
- **CONTENT:** Does it contain spelling errors or poor grammar?

1 in 101

emails contain malware

ADMINISTRATION FOR CHILDREN & FAMILIES
Office of the Chief Information Officer

Version 1.0