



P&RCIO NEWSLETTER

SERVING THE P&R COMMUNITY
VOLUME 5, ISSUE 1



FALL 2012

Personally Identifiable Information (PII): What Does it Mean?

POINTS OF INTEREST:

- PII: What Does it Mean?
- Proper Safeguards for PII

The Department of Defense (DoD) Privacy Program Directive (5400.11) states that “the privacy of an individual is a personal and fundamental right that shall be respected and protected.” The directive goes on to say that “the legal rights of individuals, as guaranteed by Federal laws, regulations, and policies, shall be protected when collecting, maintaining, using, or disseminating personal information about individuals.” Finally, “DoD personnel, to include contractors, have an affirmative responsibility to protect an individual’s privacy when collecting, maintaining, using, or disseminating personal information about an individual.” Generally, protecting privacy means protecting Personally Identifiable Information (PII). PII is defined as any information that is unique to an individual. As such, PII can identify, link, or describe a specific person, either explicitly or when paired with other available information. Common examples of PII include social security number, birth date, phone number, email address, home address, and financial information.

How is PII treated?

Not surprisingly, PII is handled carefully due to its sensitive nature. The Privacy Act serves as a regulation of the “collection, maintenance, use, and dissemination of PII.” More specifically, the Privacy Act requires the following:

- Establish rules of conduct for collecting, maintaining, distributing, and disposing of personal information
- Publish Privacy Act system of records notices in the Federal Register for all

approved collections of privacy information

- Ensure that only data authorized by law is collected and that information is shared only with those who have a need-to-know



- Establish and apply data safeguards to protect information from unauthorized disclosure
- Allow individuals to review records about themselves for completeness and accuracy and to amend any information that is in error
- Keep record of disclosures made outside of DoD

What happens when it goes wrong?

The loss of PII can lead to identity theft, which is costly to the individual and to the Government. It can impact our organizations by resulting in costly actions being taken by the organization as well as potential actions taken against the responsible individual(s). It also erodes confidence in the Government.

Sources:

DoD Privacy Program Directive:
<http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf>

Introduction to the Privacy Act:
[http://dpclo.defense.gov/privacy/documents/2011%20DPCLO Intro Privacy Act.pdf](http://dpclo.defense.gov/privacy/documents/2011%20DPCLO%20Intro%20Privacy%20Act.pdf)



Proper Safeguards for Personally Identifiable Information (PII)

Employees who handle PII must remember the importance of keeping the information protected because the damages that could result from an unauthorized release of any PII could be disastrous.

A simple but important practice is to comply with relevant System of Records Notices (SORN). A SORN is a formal notice published in the Federal Register that advises the public of data collection. SORNs also declare what data will be collected and how it may be utilized, safeguarded, and in some cases, shared; therefore, it is important for organizations and individual employees alike to refer to the SORN that corresponds to the PII in question.



Unfortunately, one good practice is not enough to assure secure maintenance of PII. It is best to take a multi-faceted approach to protecting PII, utilizing a combination of technical, administrative, and physical safeguards. The following are a few guidelines:

- Think PRIVACY when you send/receive emails that contain PII; are these messages properly marked?
- Any email messages that contain PII must

contain the proper markings AND BE ENCRYPTED!

- Think PRIVACY when you create documents; do you really need to include the PII?
- Think PRIVACY when disposing of PII; use approved cross-cut shredders
- Do NOT use interoffice envelopes to mail privacy data
- Do NOT place privacy data on shared network drives, multi-access calendars, intranet, or internet that can be accessed by individuals without an official need-to-know
- Never use personal hardware to store PII
- If you have PII on a Government-furnished laptop or notebook computer, protect the information with a password and have the computer/information encrypted
- Use locks to secure hard copy documents containing PII when stored
- Dispose of records according to schedules established in the SORN or procedures established by the National Archives and Records Administration (NARA)
- Validate that all recipients of any form of PII have a need-to-know
- SORN Managers should keep all SORNs up-to-date by reviewing them at least every two years
- Consult with to your organization's Security/Privacy Officer before collecting PII
- Report any suspected breaches immediately to your Security/Privacy Officer

Source:

Introduction to the Privacy Act: http://dpcllo.defense.gov/privacy/documents/2011%20DPCLO_Intro_Privacy_Act.pdf

