LIS SOLUTIONS MONTHLY NEWSLETTER NOVEMBER 2022

WHAT IS PERSONAL IDENTIFYING INFORMATION (PII)

Per the United States General Services Administration (GSA), PII refers to "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."

The Department of Homeland Security (DHS) has put together a helpful list of Sensitive PII which it notes includes but is not limited to:

- Social Security Numbers
- Driver's license numbers
- Alien Registration numbers
- Financial or medical records
- Biometrics, or a criminal history

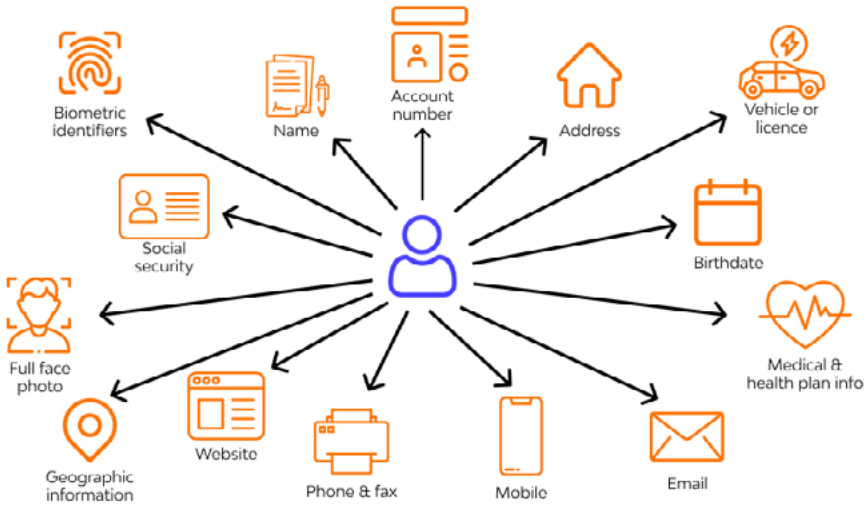
This data requires stricter handling guidelines because of the increased risk to an individual if compromised. The loss of PII can lead to identity theft which can result in financial and credit losses to individuals.

POLICIES ON PROTECTING AND SAFEGUARDING SENSITIVE INFORMATION

Because of the potential harm to individuals when PII is compromised, it is critical that threats are taken seriously and that this data is protected at all times.

Individuals having access to personal information shall respect the confidentiality of such information, and refrain from any conduct that would indicate a careless or negligent attitude toward such information.

Individuals should not permit any unauthorized viewing of records contained in any system of records. Only individuals who have a "need to know" in their official capacity shall have access to such systems of records.



LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com

RECOMMENDED TRAINING:

Identifying and Safeguarding Personally Identifiable Information (PII) Version 3.0 (usalearning.gov)

"This training starts with an overview of Personally Identifiable Information (PII), and protected health information (PHI), a significant subset of PII, and the significance of each, as well as the laws and policy that govern the maintenance and protection of PII and PHI."

"The Federal government requires the collection and maintenance of PII to govern efficiently. However, because PII is sensitive, the government must take care to protect PII, as the unauthorized release or abuse of PII could result in potentially grave repercussions for the individual whose PII has been compromised, as well as for the federal entity entrusted with safeguarding the PII."

"This training is intended for DOD civilians, military members, and contractors using DOD information systems."

Launch Course:
https://securityawareness.usalearning.gov/piiv2/index.htm

THE CYBER SIDE OF PII

Organizations must play a role in protecting PII data by establishing procedures for access control. According to Corinne Bernstein at TechTarget, " ...best practices include using strong encryption, secure passwords, and two-factor (2FA) and multifactor authentication (MFA)."

Bernstein goes on to say: "Other recommendations for protecting PII are:

- encouraging employees to practice good data backup procedures.
- safely destroying or removing old media with sensitive data.
- installing software, application, and mobile updates.
- using secure wireless networks, rather than public Wi-Fi; and
- using virtual private networks (VPNs).

To protect PII, individuals should:

- limit what they share on social media.
- shred important documents before discarding them.
- be aware to whom they give their Social Security numbers; and
- keep their Social Security cards in a safe place.

Individuals should also make sure to make online purchases or browse financials on secure HTTP Secure (HTTPS) sites; watch out for shoulder surfing, tailgating or dumpster diving; be careful about uploading sensitive documents to the cloud; and lock devices when not in use."

Bindu Sundaresan, in an AT&T blog, provides "foundational steps" to creating a protection framework for PII:

- "Understand the data: identify and classify it by source, type, sensitivity, and criticality to the business.

- Understand the threats they are exposed to due to the constantly changing nature of the threat landscape, a review of the threat exposure should be performed on a regular basis.
- Provide that the data's protection is commensurate with the threat: this means that the controls that composed the Security Framework need to be adapted to each case, so the risks are adequately mitigated."

REFERENCES:

- https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act
- https://www.dhs.gov/privacy-training/what-personally-identifiable-information
- https://www.mcafee.com/blogs/privacy-identity-protection/take-it-personally-ten-tips-for-protecting-your-personally-identifiable-information-pii/
- https://www.techtarget.com/searchsecurity/definition/personally-identifiable-information-PII
- https://cybersecurity.att.com/blogs/security-essentials/what-you-need-to-know-about-pii-security-in-2019