The Privacy Act

As providers who offer services to clients under U.S. government contracts, you have a contractual obligation to abide by the laws that protect the information you collect, process, transfer and store. One of the laws that protect this information is the Privacy Act of 1974. Please read this guidance carefully and work with your organization to ensure compliance.

What is the Privacy Act?

The Privacy Act of 1974 ("Act") is a federal law that regulates when personal information maintained in a system of records may be collected, how it may be accessed, used, and disseminated, and how it must be maintained. This portion of the training is to educate you on the provisions of the Act and how to handle and safeguard personal information. The U.S. government mandates training on this topic, to be completed before you handle personal information on behalf of an agency. The Privacy Act is not to be confused with another privacy law, the Health Insurance Portability and Accountability Act (HIPAA), which stipulates what rights patients have over their protected personal health information.

Definitions

To understand when this law applies, you must be familiar some key definitions in the Act:

- *Personally Identifiable Information (PII)* is "Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Examples of PII include name, personal phone number, social security number, date of birth, email or home mailing address, driver's license, spouse or child information, gender, security clearance, biometrics, and financial, medical or disability information.
- A *Record* is a collection of personal information about an individual.
- A *System of Records* is a group of records under agency control and which information is retrieved by an individual identifier.
- A *System of Records Notice*, *or SORN*, is the notice published in the Federal Register before an agency collects PII from an individual. It will include the information to be collected, purpose, routine uses, safeguards, storage, retention and disposal and the authority for its collection.

General rules

Personally Identifiable Information must be handled in accordance with strict guidelines under the Privacy Act and agency policies. If you are handling any such information for a federal government customer, remember that the Act requires that:

- Information about an individual that is kept in a system of records should be collected only from that individual to the greatest extent practicable.
- Information requested from the individual should be relevant and necessary to accomplish the purpose of the collection.
- Individuals should be informed upon collection of the authority to collect, purpose of the use, routine uses and effects, if any of not providing the information.

- The individual's PII may not be disclosed except by that individual's written request unless there is an exception authorizing disclosure.
- The PII maintained about an individual must be accurate, relevant, timely and complete with respect to collection, dissemination and maintenance.

In addition, there must be safeguards in place when handling PII. Continue reading below.

Handling and safeguarding PII

There are three different types of safeguards you should always practice when handling PII – administrative, physical and technical. Review further to learn more about the types of safeguards you should have in place under these types of controls.

Administrative Safeguards

Examples of administrative safeguards include:

- Policies – Persons who handle PII should have a comprehensive set of policies that address handling and safeguarding PII.
- Training – Individuals must take training that covers privacy and information security Including any customer training, including privacy training, as required under the contract.
- Privacy assessments – Persons should conduct assessments on the security of the information it handles under U.S. government contracts.

Physical Safeguards

There are several physical means for securing personal information including:

- Using a monitor privacy screen where sensitive data may be in view of unauthorized individuals.
- Securing printed information in secured storage locations such as locked cabinets when not in use, including information in plain view of an office.
- Restricting discussions of personal information in areas where it can be overheard.
- Using cover sheets for faxed records.
- Sharing personal information only with those with a "need to know."

Also, records must be retained and disposed of in accordance with requirements set forth in the SORN. PII handled under contract not covered by a SORN will be retained in accordance with the contract terms. Providers can work with Magellan program staff if there are any questions about retention periods under the contract. When records are no longer required to be retained, destruction must be tailored to the type of record (e.g., paper or electronic) and be rendered unrecognizable and beyond reconstruction. Examples include cross-shredding, burning, or deleting from all electronic folders including the recycle bin.

Technical safeguards

Technical safeguards include:

- Protecting devices, the data contained therein, and any other PII related materials from potential damage, theft, or unauthorized access.
- Implementing logical locks and password protection mechanisms to secure sensitive and highly sensitive data whenever feasible.

- Being aware that a list of U.S. government banned software also extends to personally owned devices utilized for work-related purposes.
- Not sharing devices with unauthorized users unless each user can be distinctly identified and held accountable for their activities on the devices.
- Maintaining possession of portable devices or storing them in controlled and secured locations when not in use.
- Using automatic lockout features that secure devices automatically when the user walks away without manually locking the device.

Moreover, it is essential to be mindful of additional technical safeguards, including maintaining strong passwords and being aware of phishing risks by verifying the sender's identity.

Restricted uses

Under the Act, individuals may request access their records, request copies and seek amendment of erroneous factual information.

Other disclosure of PII may not be made without written request by, or prior written consent of the individual to whom the record pertains unless disclosure is to officers and employee so the agency who have a need for the record in the performance of their duties or for an established routine use as described in the SORN.

Reporting incidents

If you are concerned that an incident, such as an unauthorized disclosure, unauthorized access, or other compromise of data involving personal information has occurred you should immediately contact MFGetEthics@MagellanFederal.com.

Penalties

There are civil as well as criminal penalties for noncompliance with of any of the provisions of the Act. Officers or employees as well as contractors who willfully disclose records may be convicted of a misdemeanor and fined up to $5,000. Civil penalties for failure to comply with the Act include payment of damages and attorney's fees.