

PRIVACY TRAINING MODULE 200



Training for Managers & Supervisors

Online Training

Privacy Basics



Privacy provides citizens and lawful aliens with guaranteed rights to:

- Access to/amendment of their records, ensuring they are accurate, timely, and complete
- To appeal agency decisions
- To sue for breaches

Why the Need for Training?



Recent breaches have brought unnecessary, negative attention to the Corps.

- ❑ Reeducation and reemphasizing personal responsibility for protecting unauthorized disclosures is needed.

- ❑ The Marine Corps must act now to:
 - Reduce and eliminate breaches
 - Emphasize personal responsibility for protecting private information.

The VA Breach has made the public skeptical of how government entities protect personal information.

Personal Data



Personal data could be but is not limited to:

- Financial, credit, and medical data
- Social Security Number
- Birthdates
- Family data
- Security clearance level
- Home addresses and telephone numbers
- Mother's maiden name; other names used
- Drug test results and the fact of participation in rehabilitation programs
- Religion, race, national origin
- Performance Ratings
- Names of employees who hold government issued travel cards, including card data

When dealing with personal information, always take a moment to think about privacy

Why is the Collection of PII Necessary?



The Marine Corps collects personal information for several reasons:

- To Hire You
- To Pay You
- To Locate You
- To Educate You
- To Provide Services to You

There is a delicate balance between maintaining official records and protecting the individuals' right to privacy.



Access to Personal Information

Ensure that you and your staff practice limited access principles

- Grant access to only those specific employees who require the record to perform specific, assigned duties
- Closely question other individuals who ask for your data

Why do they need access? How will it be used?

Collecting PII



- ❑ Agencies may not collect personal data without first publishing a System Notice in the Federal Register that announces the collection.
- ❑ The System Notice sets the rules for collecting, using, storing, sharing, and safeguarding personal data when records are retrievable by PII.

A Systems Notice informs the general public of what data is being collected, the purpose for the collection, and the authority for doing so.

Collecting PII



- If you collect it you must protect it!
- If in doubt leave it out!

**If you don't need the entire SSN, use
the last 4 digits!**

**Just because you've handled PII one way, does not mean it is
the best way**

What is a System of Records?



A System of Records is a group of records that:

- Contains a personal identifier (such as a name, Social Security Number, Employee Number, etc)
- Contains one other item of personal data (such as home address, performance rating, blood type, etc)
- Is retrieved by a personal identifier

Privacy Act Systems of Records Notices



Per the Privacy Act all Executive Branch Agencies must:

- ❑ Identify “systems of records” that allow the collection of information retrievable by a personal identifier
- ❑ Provide a Systems of Records Notices (SORN) to inform the public of what data is being collected, the purpose of collection, and the authority for doing so
 - A SORN sets the rules that the Marine Corps will follow on collecting and maintaining PII

Review Your Office Protocols



Remain aware of the databases under your control that contains personal information

- Identify the Privacy Act systems notice that permits the collection
- Properly safeguard those records
- Properly dispose of those records

Review Your Office Protocols



- Only share those records with individuals who have an official need to know

- Follow proper records management practices for maintaining or destroying those records

Your Duties as Supervisor



As a supervisor, you and your staff

- ✓ May initiate data collections
- ✓ Receive privacy data in the course of conducting business
- ✓ Create, manage, or oversee files or databases containing personal data
- ✓ Disseminate personal data



Your Duties as Supervisor

When directly soliciting PII from an individual...

- ✓ Provide the individual a Privacy Act Statement
- ✓ Identify the Privacy Act SORN that allows the collection
- ✓ Identify safeguards that you have in place to prevent inadvertent disclosures

Soliciting Data for a Recall Roster



Organizations are allowed to maintain recall rosters when collected information meets purpose statement listed in PA SORN *NM05000-2, Administrative Personnel Management System*

Soliciting Data for a Recall Roster



Civilian employees and contractors may give supervisors their home addresses and telephone numbers

- They do not have to agree to share these with co-workers
- If an employee objects to having his/her information posted on a recall roster

List their numbers as “unlisted” or “unpublished and arrange to call the employee yourself during alerts or exercises

Soliciting Data for a Recall Roster



- Properly mark the recall roster "For Official Use Only-Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties."
- Instruct your staff that recall rosters are used for official purposes only and must be kept in a secure location.

Prevent Privacy Civil Penalties



What Privacy violations may lead to civil penalties?

- Unlawfully refusing to amend a record or grant access
- Failure to maintain accurate, relevant, timely, and complete data
- Failure to comply with any Privacy Act provision or agency rule that results in an adverse effect

Transmitting PII



Do not use interoffice mail envelopes to route personal data

- Use sealable envelopes addressed to the authorized recipient

Properly mark personal data that you transmit via letter or email "For Official Use Only-Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties"

Remember to Make Privacy a Priority



- Voice your commitment to protecting PII
- Remind staff to use caution when posting Private Information
- As you move to electronic records, review established practices to determine if they are best practices

- Periodically review shared devices for compliance
- If you maintain a website, ensure that documents posted do not contain personal data
- Don't collect personal data because you *might* need it. Collect it because you *do* need it

Military and Civilian Personnel Records



Both military and civilian personnel records are Privacy Act systems of records collections

- ❑ OPM GOVT-1 governs most civilian personnel records
- ❑ MMN00006 is the PA systems notice for Marine Corps Military Personnel Records

The individual to whom these records pertain gets the entire record.

If Contractors are Working for You



- Ensure that they understand Privacy and comply with all Privacy policies
- Ensure that the contract includes the federal acquisition regulation Privacy clauses in the contract
- Ensure language in the contract addresses how data is to be disposed at the end of the contract

Prevent Privacy Criminal Penalties



What Privacy violations may lead to criminal penalties?

- Collecting data without meeting the Federal Register publication requirement
- Sharing data with unauthorized individuals
- Acting under false pretenses
- Facilitating those acting under false pretenses

Penalties include a misdemeanor charge (jail time of up to one year and/or fines up to \$5000).

Maintaining Notes



If you maintain information on your employee as personal notes to rate their performance...

- You are not required to maintain it
- Do not share it
- Do not file it in official files
- Destroy it at your convenience

Your notes are memory joggers and DO NOT qualify as an agency record; they are not subject to access by the employee

Maintaining Notes



If you are taking notes for the purpose of an intended/possible action against an employee

- They are agency records
- Records usually fall into an OPM government system
- Information is releasable to the employee in their entirety

Loss of PII



The loss of PII has major implications for the Marine Corps

- Can erode confidence in the government's ability to protect information
- Can impact our business practices
- Can lead to major legal action

The loss of privacy information can have a devastating impact on the individual and the organization.

Loss of PII (con't.)



The loss of PII has major implications for affected Marines (military, civilian, & contractor)

- Can be embarrassing
- Can cause emotional stress
- Can lead to identity theft which can be costly to both the individual and the government

The loss of privacy information can have a devastating impact on the individual and the organization.

Loss of PII (con't.)



The loss of PII has major implications for the individual(s) responsible for the loss/compromise

- Can result in disciplinary actions
- Can result in civil or criminal actions being taken against the employee
- Can result in costly fines and imprisonment

These actions could range anywhere from jail time up to one year and \$5000 in fines!

How do I protect Private Information?



First, think about the different methods that PII is stored and disseminated:

- On Hard Drives
- On Portable media
- On Paper documents
- On E-mail

Electronic methods of storage and delivery have added new concerns and vulnerabilities concerning the protection of PII.

PII on Laptops



When traveling with your laptop:

- Do not leave it unattended! Even at small stops, carry it in with you.
- While traveling through airports, take your laptop on the flight as carry on luggage.
- NEVER leave it in your vehicle.

Over 15% of breaches were due to individuals failing to properly protect their laptops from theft.

PII on Laptops (cont.)



Only DoD owned or leased laptops are authorized for storing PII data

- Will be signed in and out by a supervising official designated in writing by senior leadership.
- Configured to require certificate based authentication for logon whenever possible.
- Implement a screen lock after 15 minutes of inactivity
- Employ, at a minimum, NIST-certified, FIPS 140-2 or current encryption standards.

Read GENADMIN APR 07: Safeguarding PII for additional guidance



Personal Electronic Devices

Personal Electronic Devices (PEDs) refer to any non-stationary electronic device capable of recording, storing, and/or transmitting information.

Examples include:

- Blackberries
- Personal Digital Assistants (PDAs)
- Web based cell phones

Laptops also fall into this category.

Personal Electronic Devices



PEDs containing PII:

- Will be signed in and out by a supervising official designated in writing by senior leadership.
- Configured to require certificate based authentication for logon, whenever possible
- Implement a screen lock after 15 minutes of inactivity

Read GENADMIN APR 07: Safeguarding PII for additional guidance

PII on Thumb Drives



If you:

- Put your thumb drive in your pocket
- Drop it in your handbag
- Leave it in your computer
- Attach it to your key ring

There is a possibility that you could lose it and the data on it.

Would you know what information would be lost?

10% of the losses of PII were due to lost thumb drives.

PII on Thumb Drives (cont.)



- Do not store PII on thumb drives if it's not absolutely necessary.
- Encrypt data that is stored on thumb drives.
- Keep your thumb drive on your person at all times.

PII of any form will NOT be stored on personally owned laptops, thumb drives, or PEDs.

Posting Information



- Ensure that recall rosters are not posted in a public folder for access by individuals who DO NOT have access.
- Ensure that PII is not mistakenly posted on an intranet/internet website.
- Routinely check internet/intranet/portal sites under your purview for erroneous postings

Over 30% of breaches were attributed to such postings

Sending Information



- Determine the sensitivity of the information and the potential impact of a loss before relying on an email to share information.
- Properly mark the document to alert the reader on the necessity to protect the information.
- Provide information to the reader as to who to contact should the email be received by an unauthorized recipient.

Over 20% of reported breaches were a result of improper email practices

Disposal



Proper disposal of PII is any means of destruction that renders documents or records unrecognizable and beyond reconstruction.

□ Think twice before tossing documents in the trash or recycling containers.

“Dumpster Diving” is a cheap and easy method to gain information about an individual.

Over 20% of breaches were a result of improper disposal

Should you lose Privacy Information



- In the event of a PII loss, report it within 1 hour per direction of MARADMIN
- Failure to meet deadlines as outlined will require additional reporting

Policies can be found at the Marine Corps Privacy website at

<https://hqodod.hqmc.usmc.mil/PII.asp>

Follow the procedures indicated in the MARADMIN, but always remember to report the loss to your immediate chain of command.

Disclosure of PII



❑ The Privacy Act forbids disclosure of personal information to those who are not entitled to view or access it. This is referred to as the "No Disclosure without Consent Rule."

This is a misdemeanor charge along with a \$500 fine!!

However, there are several exceptions to this rule.

We all have a responsibility to prevent unauthorized individuals from obtaining private information.

Exception to the “No Disclosure Without Consent” Rule



5 U.S.C. § 552a(b)(1) Those officers and employees of the Agency which maintains the record who have a need for the record in the performance of their duties.

This exception authorizes the intra-agency disclosure of a record for necessary, official purposes.

Any disclosure made pursuant to this exception DOES NOT require an entry on the Accounting Disclosure Form in the applicable record

Exception to the “No Disclosure Without Consent” Rule



5 U.S.C. § 552a(b)(2) is required under 5 U.S.C § 552, as amended.

Any request citing to 5 U.S.C 552a(b)(2) will be processed as a FOIA request and will be handled and coordinated by the unit's FOIA Coordinator.

Any disclosure made pursuant to this exception **DOES NOT** require an entry on the Accounting Disclosure Form in the applicable record.

Any disclosure made pursuant to this exception DOES NOT require an entry on the Accounting Disclosure Form in the applicable record.

Exception to the “No Disclosure Without Consent” Rule



□ **5 U.S.C. § 552a(b)(3)**-requires Federal Register publication of “each routine use of the records contained in the systems, including the categories of users and the purpose of such use.”

Routine is defined in this instance to mean with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected- 5 U.S.C. § 552a(b)(7)

Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

Exception to the “No Disclosure Without Consent” Rule



□ **5 U.S.C. § 552a(b)(4)**- Exception to the Census Bureau for the purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13.

Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

Exception to the “No Disclosure Without Consent” Rule



□ **5 U.S.C. § 552a(b)(5)**-to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable.

□ **5 U.S.C. § 552a(b)(6)**-to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value.

Any disclosure made pursuant to these exceptions DOES require an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

Exception to the “No Disclosure Without Consent” Rule



□ **5 U.S.C. § 552a(b)(7)**-allows disclosure to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.

While disclosures made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record, disclosures made pursuant to this exception will NOT be made available for viewing by the subject of the record.

Exception to the “No Disclosure Without Consent” Rule



□ **5 U.S.C. § 552a(b)(8)**-allows disclosure to person pursuant to a showing of compelling circumstances affecting the health or safety of individuals if, upon such disclosure, notification of disclosure is transmitted to the last known address of the subject individual.

Any disclosure made pursuant to this exception ALSO requires an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

Exception to the “No Disclosure Without Consent” Rule



□ **5 U.S.C. § 552a(b)(9)**-allows disclosure to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee of any such joint committee.

This exception DOES NOT authorize the disclosure of a Privacy Act protected record to an individual Member of Congress acting on his/her own behalf or on behalf of a constituent.

Any disclosure made pursuant to this exception ALSO requires an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

Exception to the “No Disclosure Without Consent” Rule



□ **5 U.S.C. § 552a(b)(10)**-allows disclosure to the Comptroller General, or any of his authorized representatives, in the course of the course of the performance of the duties of the General Accounting Office.

Any disclosure made pursuant to this exception ALSO requires an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

Exception to the “No Disclosure Without Consent” Rule



□ **5 U.S.C. § 552a(b)(11)**-allows disclosure pursuant to the order of a court of competent.

An essential point of this exception is that the Privacy Act “cannot be used to block the normal course of court proceeds, including court-ordered discovery.”

Any disclosure made pursuant to this exception DOES requires an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

Exception to the “No Disclosure Without Consent” Rule



□ **5 U.S.C. § 552a(b)(12)**-allows disclosure to a consumer reporting agency in accordance with section 3711(e) of Title 31.

This disclosure authorizes agencies to disclose bad-debt information to credit-bureaus, but only after the agency has completed a series of due process steps designed to validate the debt and to offer the individual an opportunity to repay it.

Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

References



- **DoD 5400.11-R, 14 May 07**: DoD Privacy Program
- **OMB Memo 22 May 07**: Safeguarding against and responding to the breach of PII
- **ALNAV 057/07**: Safeguarding PII from Unauthorized Disclosure
- **GENADMIN Apr 07**: Safeguarding PII
- **MARADMIN 431/07**: Update to reporting process for loss or compromise of PII data
- **MARADMIN 389/07**: Disposal procedures for documents containing PII
- **MARADMIN 267/07**: Reporting process for loss or compromise of PII data

These references and much more can be found at the Marine Corps Privacy website at <https://hqodod.hqmc.usmc.mil/PII.asp>



Congratulations!

You have completed your annual PII 200 Training

[Click to Email Completion to HR](#)

Click button above to email completion to HR.

You MUST include your;

Full Name

**Employee ID Number
and Course Title**

in the body of the email.