

## What kind of personal information must I protect?

Examples include:

- ✓ Names
- ✓ Account numbers
- ✓ Certificate/license numbers
- ✓ Date and place of birth
- ✓ Dependent information
- ✓ Driver's license number
- ✓ Electronic mail addresses
- ✓ Employment history information
- ✓ Fax numbers
- ✓ Full face photographic images and any comparable images
- ✓ Health plan beneficiary numbers
- ✓ Internet Protocol (IP) address numbers
- ✓ Medical record numbers and medical history information
- ✓ Postal address information, where it would identify an individual under applicable law
- ✓ Social Security Numbers
- ✓ Telephone numbers
- ✓ Veterans Benefits Administration (VBA) claim record/folder file numbers
- ✓ Vehicle identifiers and serial numbers, including license plate numbers
- ✓ Other personal information, such as financial or education information
- ✓ Any other unique identifying number, characteristic, or code derived from, or related to, information about the individual or otherwise capable of being translated so as to identify the individual

### VA Privacy Service

The VA Privacy Service was established in 2002 to take the lead in protecting the confidentiality of veteran and employee data. We oversee all privacy efforts within VA and ensure all privacy laws and regulations are applied consistently throughout the Department. Our programs, products, policies, and procedures are developed centrally and implemented nationally by field-level Privacy Officers around the country.

### For More Information

To learn more about privacy:

- Contact your local Privacy Officer. If you do not know your Privacy Officer, ask your supervisor.
- Email specific privacy related questions to the Privacy Service at [privacy@va.gov](mailto:privacy@va.gov).
- Call the Privacy Service at 202-273-5070.

To learn more about security:

- Contact your local Information Security Officer.
- Visit the Information Assurance web page at <https://vaww.ocis.va.gov/portal/server.pt>

***Protect the privacy of personal information.***



## Respecting Privacy – Building Public Trust



**Privacy: It's Everyone's Business**

Over the past year, the Department of Veterans Affairs (VA) has experienced several privacy and data breaches involving veteran and employee information. These incidents have eroded the public's trust about the Department's commitment to protecting personal information.

VA has over 230,000 employees, maintains extensive records on more than 26 million veterans, and provides services and benefits to over 8 million veterans. As the Secretary for the Department recently stated, "We must regain the public's trust in our mission to honor and serve our veterans."

### What Can I Do to Increase Public Trust in VA?

VA is creating a culture that always puts the safekeeping of veterans' personal information first. Everyone – employees, contractors, business associates, and volunteers – needs to be committed to achieving this goal.

There are several things you can do:

- **Take your training** – Everyone must take privacy awareness training once a year. Your facility Privacy Officer will tell you which course you need to take. There is also specialized training for program managers and senior executives.
- **Understand what information you work with and/or have access to** – VA collects and maintains a wide range of veteran and employee information. **Do not assume you can use VA information any way you wish.** Talk with your supervisor to find out what you can and cannot do with the information you have and the information you want.
- **Keep information secure** – Use a screen saver on your computer when you leave your desk, log off your computer, and lock up files at the end of the day.
- **Back up your information** – Copy your electronic files on a regular basis and keep the copy in a secure place.
- **Encrypt sensitive information** – Learn how to use encryption software when sending personal information electronically. Password-

protect files on your computer if they contain personal information. Please contact your local Information Security Officer (ISO) to learn more about encryption and how to password protect your files.

- **Get rid of information you no longer need** – Shred paper documents, destroy CDs and DVDs, and delete information from your computer.
- **Be careful when telecommuting or traveling** – Only take the information you need, do not keep your passwords with your computer, use a cable lock for your laptop, and always know where your computer is and keep it safe.
- **Be extra careful when using portable storage devices** – Memory sticks, thumb drives, Blackberries, and cell phones can store a lot of information, but they can be easily lost or stolen.
- **Report all privacy and security incidents** – Report all incidents to your Privacy Officer and ISO. This includes accidental incidents, such as information left on a copier at the end of the day, and malicious incidents, such as the theft of a laptop.

### Who Has Access to Personal Information?

Do you think only doctors, nurses, and claims examiners have access to personal information? You are wrong. Almost everyone at VA has access to some employee or veteran information. But, you are only allowed to use it if you have an official need for the information. For example, managers process personnel actions and are permitted to access personnel files. Contractors service information systems that contain medical and claim information.

*However*, maintenance staff may see patient and claims information if documents are improperly discarded in the recycling bin or trash can. Volunteers may hear stories from veterans in the hospitals, but they should not repeat them.

### What Information Should I Protect?

You must protect all sensitive and personal information collected, maintained, and used by

VA. Specifically, you must protect veteran and employee information that can be used to identify a particular person. Examples are on the back of this brochure. Information in all forms is covered – electronic, paper, verbal, and other.

### How Do I Report Privacy and Security Incidents?

You must report all actual or potential incidents involving personal information to your Privacy Officer and ISO as soon as possible. You should also notify your supervisor. You must notify VA police if the incident involves the theft of computer equipment. The Privacy Officer and the ISO will report these incidents within one hour to VA's Security Operations Center (SOC). The SOC then reports them to a government-wide incident response center.

The SOC will work with the Privacy Officer and the ISO to research and resolve the incident. Depending on the seriousness of the incident, other VA organizations will get involved. These include the Inspector General and the Secretary's Office.

Exercise caution before discussing actual or potential incidents with anyone other than your supervisor, Privacy Officer, and ISO. If personal information was compromised, the SOC will work with the Secretary's Office to notify the affected individuals. If appropriate, VA will provide free credit monitoring to these individuals to limit the chances of identity theft.

### What are the penalties if I do not secure veteran and employee data, or if I do not report an incident?

There will be serious consequences.

- If a VA employee, contractor, business associate, or volunteer violates privacy or security requirements, he or she could face disciplinary, monetary, and/or criminal penalties for each violation.
- Penalties may also apply to the supervisor and to the Department.