TMS 20939 - VA Privacy Training for Personnel without Access to VA Computer Systems or Direct Access to or the Use of VA Sensitive Information

Training

The Department of Veterans Affairs, VA must comply with all applicable privacy and confidentiality statutes and regulations. One of the requirements in VA is to have all personnel trained annually on privacy requirements. "Privacy" represents what must be protected by VA in the collection, use, and disclosure of personal information whether the medium is electronic, paper or verbal.

This document satisfies the "basic" privacy training requirement for a contractor, volunteer, or other personnel **only if** the individual does not use VA sensitive information or protected health information (PHI) in any form such as electronic or paper or have access to any VA computer system such as VA Time and Attendance System (VATAS), Computerized Patient Record System (CPRS), Joint Legacy Viewer (JLV), Veterans Health Information Exchange (VHIE), Compensation and Pension Record Interchange (CAPRI).

You will find this training outlines your role and responsibility for protecting VA sensitive information (medical, financial, or educational) that you may incidentally or accidentally see or overhear.

If you have direct access to VA sensitive information or access to a VA computer system where there is protected health information such as VATAS, CPRS, JLV, VHIE or CAPRI you must take Privacy and HIPAA Focused Training (TMS 10203).

VA Privacy and Information Security Awareness and Rules of Behavior (TMS 10176) is always required to use or gain access to a VA computer system or VA sensitive information, whether or not protected health information is included. Both trainings are located within the VA Talent Management System (TMS): https://www.tms.va.gov

What is VA Sensitive Information/Data?
All Department information and/or data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes not only information that identifies an individual but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.

What is Protected Health Information?
The HIPAA Privacy Rule defines protected health information as Individually Identifiable Health Information transmitted or maintained in any form or medium by a covered entity, such as VHA.

What is an "Incidental" Disclosure?
An incidental disclosure is one where an individual's information may be disclosed incidentally even though appropriate safeguards are in place. Due to the nature of VA communications and practices, as well as the various environments in which Veterans receive healthcare or other services from VA, the potential exists for a Veteran's protected health information or VA sensitive information to be disclosed incidentally.

For example:

• You overhear a healthcare provider's conversation with another provider or patient even when the conversation is taking place appropriately.
• You may see limited Veteran information on sign-in sheets or white boards within a treating area of the facility.
• You may hear a Veteran's name being called out for an appointment or when the Veteran is being transported/escorted to and from an appointment

Safeguards You Must Follow To Secure VA Sensitive Information:
• Secure any VA sensitive information found in unsecured public areas (parking lot, trash can, or vacated area) until information can be given to your supervisor or Privacy Officer. You must report such incidents to your Privacy Officer timely.
• Don't take VA sensitive information off facilities grounds without VA permission unless the VA information is general public information, i.e., brochures/pamphlets.
• Don't take pictures using a personal camera without the permission from the Medical Center Director.
• Any protected health information overheard or seen in VA should not be discussed or shared with anyone who does not have a need to know the information in the performance of their official job duties, this includes spouses, employers or colleagues.
• Do not share VA access cards, keys, or codes to enter the facility.
• Immediately report lost or stolen Personal Identity Verification (PIV) or Veteran Health Identification Cards (VHIC), VA keys or keypad lock codes to your supervisor or VA police.
• Do not use a VA computer using another VA employee's access and password.
• Do not ask another VA employee to access your own protected health information. You must request this information in writing from the Release of Information section at your facility

What are the Six Privacy Laws and Statutes Governing VA?
1. Freedom of Information Act (FOIA) compels disclosure of reasonably described VA records or a reasonably segregated portion of the records to any person upon written request unless one or more of the nine exemptions apply.
2. Privacy Act of 1974 provides for the confidentiality of personal information about a living individual who is a United States citizen, or an alien lawfully admitted to U.S. and whose information is retrieved by the individual's name or other unique identifier, e.g. Social Security Number.
3. Health Insurance Portability and Accountability Act (HIPAA) provides for the improvement of the efficiency and effectiveness of health care systems by encouraging the development of health information systems through the establishment of standards and requirements for the electronic transmission, privacy, and security of certain health information.
4. 38 U.S.C. 5701 provides for the confidentiality of all VA patient and claimant information, with special protection for their names and home addresses.
5. 38 U.S.C. 7332 provides for the confidentiality of drug abuse, alcoholism and alcohol abuse, infection with the human immunodeficiency virus (HIV) and sickle cell anemia medical records and health information.
6. 38 U.S.C. 5705 provides for the confidentiality of designated medical-quality assurance documents.

What are the Privacy Rules Concerning Use and Disclosure?
You are not authorized to use or disclose protected health information. In general, VHA personnel may only use information for purposes of treatment, payment or healthcare operations when they have a need-to-know in the course of their official job duties. VHA may only disclose protected health information upon written request by the individual who is the subject of the information or as authorized by law.

How is Privacy Enforced?
There are both civil and criminal penalties, including monetary penalties that may be imposed if a privacy violation has taken place. Any willful negligent or intentional violation of an individual's privacy by VA personnel, contract staff, volunteers, or others may result in such corrective action as deemed appropriate by VA including the potential loss of employment, contract, or volunteer status. Know your VA/VHA Privacy Officer and Information Systems Security Officer. These are the individuals to whom you can report any potential violation of protected health information or VA sensitive information, or any other concerns regarding privacy of VA sensitive information.

YOU ARE RESPONSIBLE FOR PROTECTING THE CONFIDENTIAL INFORMATION OF OUR VETERANS

_____ _____
Employee (Print Name) Date

_____
Employee Signature

_____
Print Name of Contract Agency, if contractor

_____
Print Name of VHA Department/Supervisor/Contracting Officer

PROVIDE A COPY OF THIS FORM TO YOUR SUPERVISOR/CONTRACTING OFFICER FOR DATA ENTRY INTO TALENT MANAGEMENT SYSTEM