



VHA Privacy and HIPAA Training FY2013

Course Overview

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA). Revisions have been made public and the full implementation of the rule became effective April 14, 2003.

The Interim Final Rule for Breach Notification for Unsecured Protected Health Information, issued pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act, was published in the Federal Register on August 24, 2009, and became effective on September 23, 2009.

VHA has revised its policies and procedures to reflect both the changes to HIPAA and to the HITECH Act.

Goal Statement and Audience

The goal of this training is to provide knowledge of:

- The Privacy Act
- Freedom of Information Act (FOIA)
- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- The confidentiality statutes, and
- Privacy policies

Audience

The audience for this training is any employee (which includes volunteers, students, research staff, or contracted workers) who has direct access to PHI or VHA computer systems.

Employees who do not have access to VHA computer systems or PHI as a part of their job must take the combined privacy and security training *VA Privacy and Information Security Awareness and Rules of Behavior* (VA 10176) to satisfy their privacy requirement.

All employees are required to complete Privacy Training annually on their anniversary date from the previous year.



Module 1 - Basic Privacy Statutes and Regulations

Course Objectives

Upon completion of this training you will be able to identify the following:

- The background and scope of applicable privacy and confidentiality statutes and regulations,
- Rights granted to Veterans by the Privacy Act, HITECH and HIPAA Privacy Rule,
- Disclosure purposes that do not require authorization from the Veteran,
- Disclosure purposes that require authorization from the Veteran,
- Information that can be used and disclosed,
- Requirements relating to the release of information,
- Virtual Lifetime Electronic Record (VLER) and;
- Elements of the Freedom of Information Act (FOIA).



NOTE:

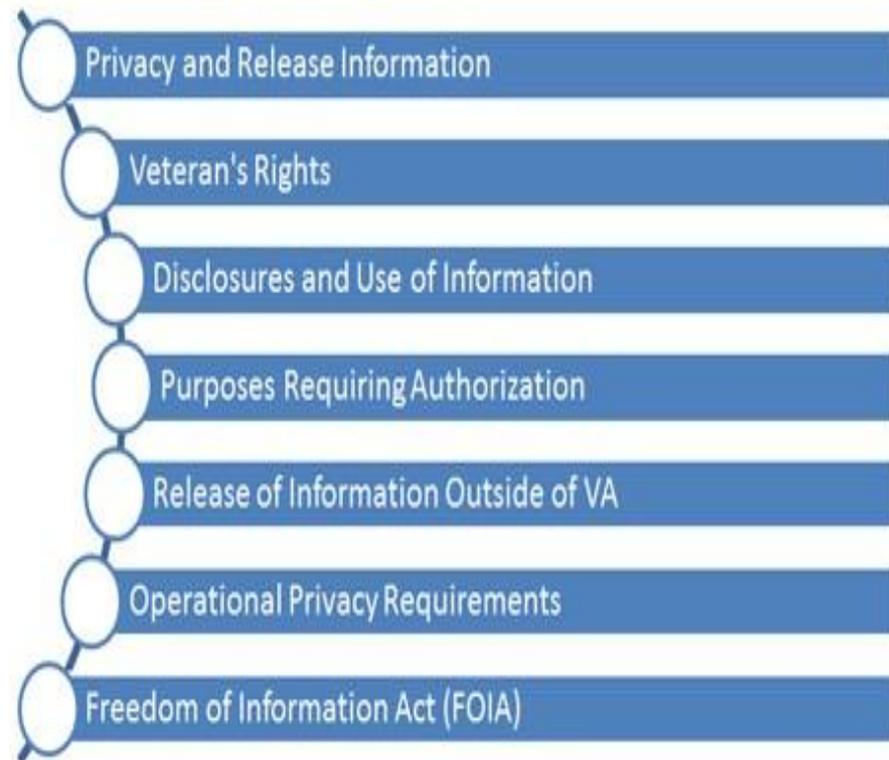
It is important to mention that this Privacy and HIPAA training course is not designed to cover topics such as breach notification, or topics that are specific to the administrations. This training is designed to be very high level but still able to cover the privacy requirements. For additional information on these topics contact your administration or VHA health care facility Privacy Officer.



Course Content

The training is organized into eight (8) modules. It is recommended to take the modules in sequential order.

1. Privacy and Release of Information
2. Veteran's Rights
3. Disclosures and Use of information
4. Purposes Requiring Authorization
5. Release of Information Outside of VA
6. Operational Privacy Requirements
7. Freedom of Information Act (FOIA)
8. Course Summary



Introduction

In this module, you will learn about the background and scope of applicable privacy and **confidentiality statutes** and regulations. Specifically you will learn the following:

- Six statutes that govern the collection, maintenance and release of information from Veterans Health Administration (VHA) records, and
- Employee's responsibilities:
 - **Use and disclosure** of information and
 - **Safeguards** under the privacy regulations.

VHA Handbook 1605.1, *Privacy and Release of Information*, establishes guidance on privacy practices and provides VHA policy for the use and disclosure of protected health information and individuals' rights in regards to VHA data. When following VHA privacy policies, all six statutes are to be applied simultaneously.

VHA health care facilities should comply with all statutes so that the result will be application of the most stringent provision for all uses and/or disclosures of data and in the exercise of the greatest rights for the individual.

- **The Freedom of Information Act (FOIA)**, 5 U.S.C. 552
- **The Privacy Act (PA)**, 5 U.S.C. 552a
- **Confidentiality Nature of Claims**, 38 U.S.C. 5701
- **Confidentiality of Certain Medical Records**, 38 U.S.C. 7332
- **Confidentiality of Healthcare Quality Assurance Review Records**, 38 U.S.C. 5705
- **The Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulation the HIPAA Privacy Rule**



Compliance

All employees shall comply with all Federal laws, regulations, VA and VHA policies. Employees shall conduct themselves in accordance with the Rules of Behavior concerning the disclosure or use of information. The VA Rules of Behavior are delineated in VA Handbook 6500, "Information Security Program," Appendix G.

Employees who have access to VHA records or VHA computer systems shall be instructed on an ongoing basis about the requirements of Federal privacy and information laws, regulations, VA and VHA policy. Employees' access or use of PHI is limited to the **minimum necessary** standard of information needed to perform their official job duties. See VHA Handbook 1605.2, "Minimum Necessary Standards for Protected Health Information" for additional guidance.

The Privacy Act requires that information about individuals that is retrieved by a personal identifier or other unique identifier such as Social Security Number (SSN) may not be collected or maintained until proper notifications are given to Congress, the Office of Management and Budget (OMB), and published in the Federal Register under a **VA System of Records**. A Privacy Officer or Privacy Liaison is designated at each Veterans Integrated Service Network (VISN), VA Medical Center (VAMC), VA Health Care System (VAHCS) or VHA Program Office to assist in addressing system of records questions.



De-Identified Information

De-identified information is not considered to be individually identifiable; therefore, the provisions of the Privacy Act, HIPAA, and VA confidentiality statutes do not apply. VHA may disclose de-identified information under FOIA and must be processed by the FOIA Officer.

VHA considers health information not individually identifiable only if:

- An experienced statistician determines the risk that the information can be used to identify an individual is very small, or
- Identifiers of the individual or of relatives, employers or household members of the individual are removed from the information.



NOTE:

Scrambling of names and Social Security Numbers IS NOT considered de-identified health information.



Use of Information, Part 1 of 2

All employees must use or access information only as legally permissible under applicable confidentiality and privacy laws, regulations, and policies.

All employees can use health information contained in VHA records in the official performance of their duties for treatment, payment, or health care operations purposes. However, employees must only access or use the minimum amount of information necessary to fulfill or complete their **official duties**. The minimum amount of information does not apply to treatment of an individual.



NOTE:

[Per Office of General Counsel (OGC) Advisory 80-90]– There is NO authority under the HIPAA Privacy Rule for the disclosure of a VHA employee's VAMC medical record to management or personnel officials for disciplinary investigation purposes without prior written authorization.



NOTE:

There is NO authority for an employee to access another employee's / Veteran's health record unless it is in performance of their official duties and it is for treatment, payment or health care operations. You must have an authorization or other legal authority (e.g., waiver of HIPAA authorization for research) in order to access for any other reason. Browsing an employee's /Veteran's health record for personal reasons or out of curiosity is strictly prohibited. Appropriate disciplinary action may be taken by the supervisor with guidance from Human Resources.



Use of Information, Part 2 of 2



NOTE:

It is not permitted to use VA access to provide a Veteran's PHI to an outside attorney in support of an employee's personnel grievance. It is also not permitted to share a Veteran's PHI with the Union or the Employee Equal Opportunity Commission (EEOC) in support of a personnel grievance as this becomes a privacy violation. If EEOC or the Union requires a Veteran's PHI to support an employee's personnel grievance, they will contact the VHA health care facility Privacy Officer or the ROI department.

The use of health information for other purposes such as research requires additional authority, a Veteran's written authorization, or a [waiver of HIPAA Authorization by the Institutional Review Board \(IRB\)](#). VHA employees may use a [limited data set](#) for the purpose of research, public health, or health care operations.

Contact the VHA health care facility Privacy Officer or the VHA Privacy Office for guidance on limited data sets.



Disclosure of Information

VHA employees can disclose PHI from official VHA records only when:

- VHA has first obtained the prior written authorization from the individual whom the information pertains to, or
- Other legal authority permits the disclosure without written authorization.

PHI should be disclosed to requestors with the understanding that the information is confidential and should be handled with appropriate sensitivity.

VHA may disclose PHI related to VHA treatment of drug abuse, alcoholism, and sickle cell anemia, and testing or treatment for HIV **only** when 38 U.S.C. Section 7332 also permits the disclosure. A non-VHA health care provider cannot receive 38 U.S.C. 7332 information without a specific authorization unless it is a **bona fide medical emergency**.

Examples of "other legal authority" are covered in the following modules and outlined within VHA Handbook 1605.1, "*Privacy and Release of Information*." When in doubt, always contact your local VHA health care facility Privacy Officer.



Safeguards

All employees shall ensure appropriate controls are followed to safeguard PHI from loss, defacement, tampering and to ensure the confidentiality of information.

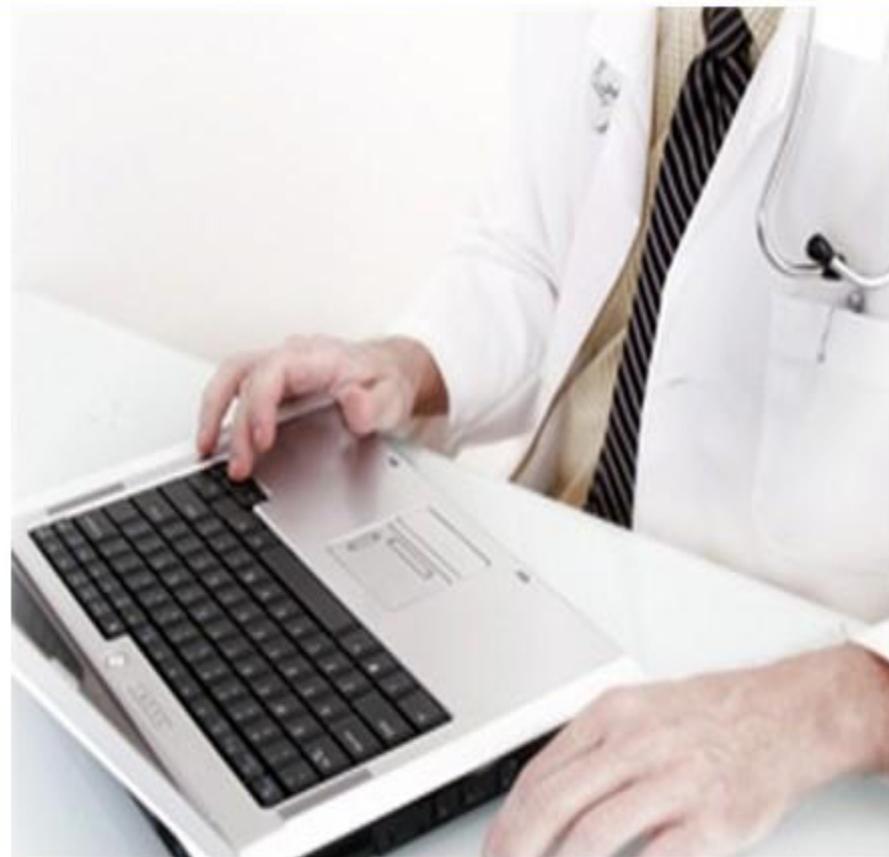
Some administrative, technical and physical safeguards are listed below. For additional information, see VA Handbook 6500 or contact your local Information Security Officer (ISO).

Access Control Policy and Procedures

- Policy for password length and complexity.
 - Example would be that a password needs to be a given length and contain certain characters.

Account Management

- Policy for account limitations and access.
 - This would be the policy that may limit the size of an account or the expiration of the account



Safeguards - Physical and Environmental Protection

Physical and Environmental Protection

- Policy for existence of locking mechanisms, fire protection, safety devices etc.
 - Doors that automatically lock behind the entrance of an authorized individual, or the installation of alarms.

Policy and Procedures

- Policies that set forth the installation and use of the above protection devices.
 - Directions for using entry control such as "no piggy-backing,"
 - Directions for activation of alarms.

Physical Access Authorizations

- Process of determining what individuals or groups should have authorized access to a given area.
 - Access control mechanism would be set to allow access-based privileges to a surgical suite.

Physical Access Control

- The method utilized to control access to an area.
 - Bio Metric devices, Card Key Access, Personal Identity Verification (PIV) Card, etc.



Safeguards - Technical

Identification and Authentication Policy and Procedures

- Policy that would delineate the requirements for access.
 - Identification used to grant access to a system known as a user name and the authentication that may be a password, or a PIV card.

Identification and Authentication (Organizational Users)

- The policy that would control access at various levels within organizations.
 - Policy that allows the surgical department access to an individual's health record.

Device Identification and Authentication

- The instructions for allowing devices to access another device.
 - Devices within a domain that would be authorized to access another device or file using an approved authentication such as a password.
 - Imaging device having access to Computerized Patient Record System (CPRS)

Summary - Module 1

Congratulations! You have completed Module 1.

In this module, you learned about

- The six statutes that govern the collection, maintenance, and release of information from VHA records, and
- The scope of privacy regulations
- Employee responsibility in the use and disclosure of information

In Module 2, you will learn about Veteran's Rights and you will have some opportunities to test your knowledge in scenario-based settings.



Module 2 - Veteran's Rights

Module 2 Introduction

In this module you will learn about the rights granted to Veterans by the Privacy Act and the HIPAA Privacy Rule. When the Privacy Act and the HIPAA Privacy Rule are in conflict, the regulation that grants the Veteran the most rights is used.

Specifically, you will learn about the Veteran's right to:

- A Notice of Privacy Practices (NoPP)
- A copy of their own Protected Health Information,
- Request an amendment to health records,
- Request an Accounting of Disclosure,
- Request and receive confidential communication,
- Request restriction of use or disclosure of records
- File a complaint



Notice of Privacy Practices (NoPP)

A Veteran or Non-Veteran receiving treatment has the right to receive a copy of the VHA Notice of Privacy Practices (NoPP). All newly registered Veterans are mailed a Notice of Privacy Practices by the Health Eligibility Center (HEC). The VHA Privacy Office is responsible for updating the NoPP and ensuring Veterans are provided the NoPP every three years or when there is a significant change. The Veteran has a right to request a copy of the NoPP from their local VHA Health Care facility at any time. The Veteran's request for a copy of the NoPP does not need to be in writing.

This notice includes the uses and disclosures of his/her protected health information by VHA, as well as, the Veteran's rights and VHA's legal responsibilities with respect to protected health information. There is one NoPP for all of VHA.

A copy of the NoPP as well as answers to questions about the NoPP and information on Non-Veteran requirements for the NoPP can be obtained from the VHA health care facility Privacy Officer or at the following website:

http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1089.



DEPARTMENT OF VETERANS AFFAIRS
VETERANS HEALTH ADMINISTRATION
WASHINGTON DC 20420

NOTICE OF PRIVACY PRACTICES

EFFECTIVE DATE APRIL 14, 2009

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED OR DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

The Department of Veterans Affairs (VA) Veterans Health Administration (VHA) is required by law to maintain the privacy of your protected health information and to provide you with notice of its legal duties and privacy practices. VHA is also required to abide by the terms of this notice and its privacy policies.

How VHA May Use or Disclose Your Health Information

Federal law allows us to use or disclose your health information *without your permission* for the following purposes:

- Treatment (e.g., giving information to VHA and other doctors and nurses caring for you)
- Eligibility and Enrollment for VA Benefits (e.g., giving information to officials who decide benefits)
- Public Health Activities (e.g., giving information about certain diseases to government agencies)
- Research Activities (e.g., giving information to a researcher to prepare a research protocol)
- Abuse Reporting
- Payment (e.g., giving information to non-VHA facilities that provide care or services)
- Patient Directories (e.g., publishing basic information about patients)
- Law Enforcement
- Judicial or Administrative Proceedings
- National Security Matters
- Correctional Facilities and/or Parole Officers
- Workers' Compensation Cases (e.g., giving information to
- Health Care Operations (e.g., giving information to individuals conducting Quality of Care reviews)
- Coroner or Funeral Activities
- When Required by Law
- Health Care Oversight (e.g., giving information to the Office of Inspector General or a Congressional Committee)
- Health or Safety Activities
- Military Activities (e.g., giving information to the Department of

Right of Access

A Veteran has a right to obtain a copy of his or her own health record. A Veteran's request must be submitted in writing to the VHA health care facility where the record is maintained and must be signed. Veterans may gain access to any information pertaining to them that is contained in any system of records.

All requests for copies will be delivered to, and reviewed by, the VHA health care facility Privacy Officer. VHA employees should refer all requests from Veterans for copies of their records to the Release of Information (ROI) Office or to another appropriate office that has a mechanism in place to track those disclosures. Clinical providers may disclose patient information at Point of Care if it's for **educational purposes**. Veteran's requesting copies of their health records must provide sufficient information to verify their identity, e.g., driver's license or other picture identification, to ensure appropriate disclosure.

If the Veteran is requesting copies of their health records by mailing in a request, a comparison of the signature on the request to a signature on file must be done prior to the disclosure of the health records.

VHA health care facilities are to process all requests for review or copies of PHI within 20 work days of receipt whenever possible. Records may be provided to Veterans on any medium.



NOTE:

Information provided via CD-ROM directly to the Veteran does not require encryption. Please refer to VA Directive 6609, "Mailing of Sensitive Personal Information."



Right to Request an Amendment

The Veteran has the right to request an amendment to any information in their health record. The request must be in writing and adequately describe the specific information the Veteran believes to be inaccurate, incomplete, irrelevant, or untimely, and the reason for this belief. The written request should be mailed or delivered to the VHA health care facility that maintains the record. The VHA health care facility Privacy Officer will review and process the request within 30 work days.



Right to an Accounting of Disclosures

A Veteran may request a list of all written disclosures of information, from his/her records. VHA facilities and programs are required to keep an accurate accounting for each disclosure made to any person or to another agency. An accounting is **not** required to be maintained in certain circumstances, including when disclosure is to VHA employees who have a need for the information in the performance of their official duties or pursuant to a FOIA request.

The request for an accounting of disclosures must be in writing and adequately identify the VA system of records for which the accounting is requested. The request for the accounting should be mailed or delivered to the VHA health care facility that maintains the record. A request for an accounting of disclosures should be delivered to the VHA health care facility Privacy Officer or designee for processing. An accounting of disclosure must be retained for 6 years after the date of disclosure or for the life of the record, whichever is longer.

Facilities should ensure that all disclosures are accounted for using the ROI Manager Software. Departments that make individual disclosures—i.e., Social Work, Prosthetics, MCCF, etc.—should utilize an electronic spreadsheet to keep track of these disclosures.

 Department of Veterans Affairs	
ACCOUNTING OF RECORDS/INFORMATION DISCLOSURE UNDER PRIVACY ACT	
1. FILE RECORD NO. (if applicable)	
2. NAME OF INDIVIDUAL TO WHOM THE RECORD/INFORMATION PERTAINS	
3. DATE OF DISCLOSURE	
4. NATURE OF DISCLOSURE (include brief description of each type of document record disclosed)	
5. PURPOSE OF DISCLOSURE	
6. NAME AND ADDRESS OF PERSON OR AGENCY TO WHOM DISCLOSURE IS MADE	7. AUTHORITY FOR RELEASE OF INFORMATION (in authority or applicable number and etc.)
8. NAME AND TITLE OF VA EMPLOYEE MAKING THE DISCLOSURE	

VA FORM 5572
JUN 2004

AdobeFormsDesigner

Right to Confidential Communications

A Veteran may request a list of all written disclosures of information, from his/her records. VHA facilities and programs are required to keep an accurate accounting for each disclosure made to any person or to another agency. An accounting **is not** required to be maintained in certain circumstances, including when disclosure is to VHA employees who have a need for the information in the performance of their official duties or pursuant to a FOIA request.

The request for an accounting of disclosures must be in writing and adequately identify the VA system of records for which the accounting is requested. The request for the accounting should be mailed or delivered to the VHA health care facility that maintains the record. A request for an accounting of disclosures should be delivered to the VHA health care facility Privacy Officer or designee for processing. An accounting of disclosure must be retained for 6 years after the date of disclosure or for the life of the record, whichever is longer.

Facilities should ensure that all disclosures are accounted for using the ROI Manager Software. Departments that make individual disclosures—i.e., Social Work, Prosthetics, MCCF, etc.—should utilize an electronic spreadsheet to keep track of these disclosures.



Right to Request a Restriction

The Veteran has the right to request VHA to restrict its use or disclosure of PHI to carry out treatment, payment, or health care operations. The Veteran also has the right to request VHA to restrict the disclosure of PHI to the next of kin, family, or significant others involved in the individual's care. This request must be **in writing** and signed by the Veteran.

VHA **is not required** to agree to such restrictions, but if it does, VHA must adhere to the restrictions to which it has agreed. All requests that the VHA health care facility Privacy Officer considers granting are to be referred to the VHA Privacy Office for consultation.

On occasion, a provider may be told a Veteran requests the sharing of information to be restricted from a family member. If this happens, the provider must send the individual to the Release of Information Officer so that they can submit their restriction request in writing. The VHA health care facility Privacy Officer will consult with the VHA Privacy Office for approval of a restriction request. Providers are prohibited from granting any verbal restriction requests. Documenting in the CPRS health record does not constitute a restriction request.

Right to Opt Out of Facility Directory

A Veteran has the right to opt-out of the facility directory. The facility directory is used to provide information on the location and general status of a Veteran. Veterans must be in an inpatient setting in order to opt-out and thus it does not apply to the emergency room or other outpatient settings. If the Veteran opts out of the facility directory no information will be given unless required by law. The Veteran will not receive mail or flowers. If the Veteran has opted out of the directory visitors will only be directed to the Veteran's room if they already know the room number.

If the Veteran is admitted emergently and medically cannot give their opt-out preference, the provider will use their professional judgment and make the determination for the Veteran. This determination may be based on previous admissions, or by a family member who is involved in the care of the Veteran. When the Veteran becomes able to make a decision, he or she is required to be asked about opting out of the facility directory.



Right of Personal Representative to a Deceased Veteran's Health Record

Employees must protect PHI about a deceased individual in the same manner and to the same extent as that of living individuals for as long as the records are maintained. Even though the Privacy Act expires upon death of the individual, the HIPAA Privacy Rule does not

The personal representative of a deceased individual (e.g. Executor of the Estate) has the same rights as the deceased individual. Employees must disclose the PHI of the deceased individual, under the right of access provisions, to the personal representative. A personal representative may also request amendments to the deceased individual's records. The next of kin may be considered the personal representative of a deceased individual.



Summary - Module 2

Congratulations! You have completed Module 2.

In this module you learned about

- The rights granted to Veterans,
- The rights of Personal Representatives for deceased Veterans.

In the next module, Uses and Disclosures within VA, you will learn about

- Uses of PHI for treatment, payment and health care operations,
- Disclosures for purposes other than treatment, payment and/or health care operations,
- Disclosures for research purposes,
- Incidental disclosures,
- System of Records (SOR)
- The process of release of information from non-VHA Systems of Records.



Module 3 - Introduction to Uses and Disclosures of Information within VA

Module 3 Introduction

In this module, you will learn about the use and disclosure purposes for release of PHI within VA that do not require a written authorization from the Veteran.

Specifically you will learn:

- Using PHI for treatment, payment and/or health care operations (TPO),
- Disclosing PHI for TPO,
- Disclosure of PHI without an authorization for other than TPO
- Compensated Work Therapy (CWT)
- Employee Access to PHI
- Disclosing PHI for research purposes,
- Incidental Disclosures,
- Logbooks,
- Systems of Records, and
- Release of Information from Compensation and Pension (C&P) Records



Using PHI without an authorization for treatment, payment, or health care operations

VHA employees may use PHI on a need to know basis for their official job duties for purposes of **treatment, payment and/or health care operations**.

- VHA may disclose PHI to DoD (for treatment purposes, including 38 USC 7332)
- VHA may disclose PHI, **excluding 38 USC 7332** Protected information, to non-VA health care providers (e.g. physicians, hospitals, clinics, and nursing homes) for treatment purposes. An accounting of disclosures is required to be maintained.
- VHA may disclose PHI, **excluding 38 USC 7332** to an insurance company for payment purposes. An accounting of disclosures is required to be maintained.



Disclosure of PHI without an authorization for other than treatment, payment, or health care operations, Part 1 of 2

For the purpose of determining a veteran's eligibility, entitlement, and/or provision of benefits, VHA may disclose Veteran PHI to the following groups:

- Veterans Benefits Administration (VBA)(under the laws administered by the Secretary of VA)
- National Cemetery Administration (NCA)(under the laws administered by the Secretary of VA)
- Board of Veterans Appeals (BVA)(under the laws administered by the Secretary of Health)
- VA contractors (as long as there is a business associative agreement in place)



Disclosure of PHI without an authorization for other than treatment, payment, or health care operations, Part 2 of 2

VHA may disclose all VHA information, to the Office of General Counsel (OGC) and Regional Counsels (RC) for any official purpose authorized by law. Neither the OGC nor RC is required to provide a written request for VHA information.

VHA may disclose PHI, except for 38 USC 7332 protected health information, to the VA Office of Inspector General (OIG) for law enforcement purposes. VA OIG is required to provide a written request for Veteran information for law enforcement purposes. For health care oversight activities a written request is not required and VHA may **only** disclose 38 USC 7332 protected health information to the OIG for health care oversight activities.

VHA may disclose PHI to VA Unions, in the course of fulfilling their representational responsibilities. VA Unions may make a request to management for copies of facility records pursuant to its authority under 5 USC 7114 (b)(4) Unions may request any records that are maintained by VHA facilities. This might include:

- releasable portions of completed administrative investigation boards (AIB),
- patient health records, and/or
- an employee's personnel records

However, under extremely limited circumstances, in accordance with 5 USC 7114 (b)(4), the Unions may be legally entitled to PHI or information protected by other statutes such as the Privacy Act

On any such request made by the Union and received by the facility, the local facility human resources must be consulted.

VHA may disclose PHI to VA Police when VHA believes the information constitutes evidence of criminal conduct that occurred on VHA grounds. VHA may disclose a picture of a Veteran to the VA Police when help is needed to locate a missing person.



Compensated Work Therapy (CWT)

Compensated work therapy (CWT) workers are considered **patients** – **NOT EMPLOYEES** – therefore they cannot be given access to Veteran PHI which is maintained by VHA. This includes computer systems and verbal or written access to PHI. Appropriate placement for these workers would be in positions with no access to PHI, which may include such areas as engineering, Acquisitions Material Management (AMM&S) groundskeeper, canteen/limited food service, and mail room mail sorter.

RESUMES and Job Applications

CWT officials can fill out job applications and resumes for the CWT worker. When an application or resume is kept for future job placement etc, it must be secured in a locked file cabinet or secured on a share point site with restricted access. The completed job application or resume cannot be mailed using Outlook unless encryption is used.

CWT workers cannot waive the security requirements required by FISMA or VA security policy for emailing using outlook. A CD can be used to mail the CWT worker their resume or job application and the CD is not required to be encrypted nor does it need to be sent via FedEx or other special mailing venue.



NOTE:

These individuals cannot have background checks completed or take privacy or security training to grant employee status.

Refer to Memorandum dated November 8, 2000 for additional guidance regarding CWT workers.

Employee Access to PHI

Since April 14, 2003 with the implementation of the [HIPAA Privacy Rule](#), supervisors can no longer access their employee Veterans' health records under a "need to know." Employee's access to PHI is limited to treatment, payment or health care operations (TPO). There is no authority under the HIPAA Privacy Rule to access an employee's health record without their authorization for employment purposes. The ability to access PHI **does not** constitute authority.



Research

VHA is one legal entity, so as a **covered entity** (both as a health plan and health care provider) the HIPAA Privacy Rule always applies to VHA employees in the performance of their official VA duties, including **VA research**, that involve the use of protected health information. All Veteran and patient information collected and maintained by VHA in a Privacy Act system of records is protected health information. Any action to collect, obtain, use, and view or access Veteran or patient information in the role as a VHA employee will be subject to HIPAA Privacy Rule requirements.

For research studies the following requirements may apply:

- **De-identification** must take place by removing the 18 HIPAA elements.
- PHI is compiled into a **limited data set** and only disclosed by using a **data use agreement (DUA)**.
- Written authorization is received from the research subject.
- Approval of Waiver of HIPAA Authorization is received from the Institutional Review Board (IRB) or **Privacy Board**.
- Activity qualifies as "**preparatory to research.**"



Preparatory to research on human subjects, a VA researcher may access PHI without the subject's written authorization. Only aggregate data will be recorded in the researcher's file and no PHI will be removed from VHA during the preparatory phase.

Further use or disclosure of PHI requires IRB approval of the research protocol, **informed consent**, or **waiver of informed consent**. In addition, the Principal Investigator (PI) must have an approved HIPAA authorization that is approved by the VHA health care facility Privacy Officer or a waiver of the HIPAA authorization by the IRB or Privacy Board. If the research involves pictures or voice recordings for other than treatment purposes, an additional VA Form 10-3203 *Consent for Use of Picture and/or Voice* is required.



NOTE:

The IRB cannot waive the VA Form 10-3203 as this is a Joint Commission requirement.

All research with in VA must be conducted by a VA employee investigator and this information is the property of the VA and not the Principal Investigator.

For non-VA research participants, a NoPP must be provided and a signed acknowledgement of VAF 10-0483 must be kept.

For additional guidance on research, see VHA Directive 1200 *Veterans Health Administration Research and Development Program* and related 1200 series handbooks and directives.

Incidental Disclosures

Many customary health care communications and practices play an important or even essential role in ensuring that Veterans receive prompt and effective health care. Due to the nature of these communications and practices, as well as the various environments in which Veterans receive health care or other services from VHA, the potential exists for a Veteran's health information to be disclosed incidentally. For example:

- A hospital visitor may overhear a provider's confidential conversation with another provider or a patient.
- A patient may see limited information on sign-in sheets.
- A Veteran may hear another Veteran's name being called out for an appointment.
- A Veteran may see limited information on bingo boards or white boards.

Incidental disclosures are permitted as long as reasonable safeguards to protect the privacy of the information are followed.

Reasonable safeguards will vary from VHA facility to VHA facility depending on factors, such as the size of the facility and the space that it has to use. In implementing reasonable safeguards, facilities should analyze their own needs and circumstances, such as the nature of the protected health information it holds, and assess the potential risks to the Veteran's privacy. VHA health care facilities should take into account the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards.



Many health care facilities providers and professionals have long made it a practice to ensure reasonable safeguards are in place for Veterans PHI. For instance:

- Speaking quietly when discussing a patient's condition with family members in a waiting room or other public area;
- Avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;
- Only using last four digits of SSN on bingo boards; and
- Using Veterans ID card for identification of the patient, when it is available.

Unauthorized disclosures are often a result of negligence, mistakes or failures to follow reasonable safeguards.



NOTE:

Lack of training is not a valid excuse for unauthorized disclosures resulting from failure to follow the reasonable safeguards required for incidental disclosures.

Logbooks

Paper logbooks can only be maintained for a compelling existing business need as approved by the VHA facility. For additional information, contact your facility health care Privacy Officer and your information security officer (ISO).

Every effort must be made to make the logbook electronic and secure on systems with appropriate IT security controls.

System of Records

A System of Records (SOR) is a group of records under the control of the agency from which PHI about an individual maybe retrieved by the name of the individual or by some other unique identifier or symbol.

- An advance public notice known as the System of Records Notice (SORN) must be published prior to an agency collecting PHI for a new SOR.
- Publication in the Federal Register is required to provide an opportunity for the interested person to comment.
- One SOR that is familiar in VHA is 24VA10P2—Patient Medical Records—VA.
- Within the SOR, there is a section describing routine uses (RU), which is a term that is unique to the Privacy Act and means the disclosure of a record outside of VA for a reason compatible with the purpose for which it was collected.
- A "routine use" gives authority to allow for disclosure outside of VA without authorization.
- For additional information on System of Records, contact your administration or VHA health care facility Privacy Officer.



For a list of all VHA systems of records go to <http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm>. You will only be able to access this address through the VA Intranet.

Release of Information from Compensation and Pension (C&P) Records

In VHA health care facilities, there are departments that are responsible for C&P exams. If these C&P exams are included in the Veteran's health record, these are to be disclosed under a first-party right of access request.

If the C&P exams are not part of the Veteran's health record, the request for the C&P exam must be referred to VBA for processing.

VHA health care facility Privacy Officers should work with these offices to determine how to process such requests. For additional information on amending C&P exams, please review VHA Directive 2010-024 "Changes in Compensation and Pension Examination Reports".

The screenshot shows the VA Compensation and Pension Service website. At the top, there is a navigation bar with the following links: Home, Veteran Services, Business, About VA, Media Room, and Location. The VA Department of Veterans Affairs logo is on the right. Below the navigation bar, the main heading reads "Compensation and Pension Service" in large blue letters. Underneath, a welcome message says "Welcome to the Compensation & Pension (C&P) Service website." The page is divided into two main columns. The left column is titled "Veterans and Servicemembers" and contains a list of services: Pre-Discharge Program, Disability Compensation, Disability Pension, Specially-Adapted Housing Grant, and Auto Grant with Adaptive Equipment. The right column is titled "Dependents of Living Veterans" and contains a list of services: Survivors and Dependents' Assistance and Monthly Payments to Children with Spina Bifida or Other Congenital Defects.

VETERANS AFFAIRS

Home Veteran Services Business About VA Media Room Location

Compensation and Pension Service

Welcome to the Compensation & Pension (C&P) Service website.

Veterans and Servicemembers	Dependents of Living Veterans
<ul style="list-style-type: none">▪ Pre-Discharge Program▪ Disability Compensation▪ Disability Pension▪ Specially-Adapted Housing Grant▪ Auto Grant with Adaptive Equipment	<ul style="list-style-type: none">▪ Survivors and Dependents' Assistance▪ Monthly Payments to Children with Spina Bifida or Other Congenital Defects

Summary - Module 3

Congratulations! You have completed Module 3.

In this module, you learned about:

- Using PHI for treatment, payment and/or health care operations (TPO),
- Disclosing PHI for TPO,
- Disclosure of PHI without an authorization for other than TPO
- Compensated Work Therapy (CWT)
- Employee Access to PHI
- Disclosing PHI for research purposes,
- Incidental Disclosures,
- Logbooks,
- Systems of Records, and
- Release of Information from C&P Records

In the following module, Purposes Requiring an Authorization, you will learn about:

- When written authorization is necessary for disclosure of information,
- Processing a request,
- Handling of disclosures and releases requiring authorization,
- Taking video, photography and voice records.



Module 4 - Purposes Requiring Authorization

Module 4 Introduction

In this module, you will learn the disclosure purposes for release of protected health information (PHI) that require written authorization from the Veteran.

Specifically, you will learn:

- Consent versus Authorization.
- When a written authorization is necessary for the disclosure of information.
- How to process a request.
- Identify various types of disclosures and releases requiring authorization.
- Taking of video, photographs and voice recordings requiring consent.



Documents Providing Written Permission Authorizing Disclosures for a Specific Purpose

An authorization as defined by the HIPAA Privacy Rule is an individual's written permission for a covered entity to use and disclose protected health information (PHI).

A "consent" is approval or permission as to some act or purpose, and is a much broader concept than authorization. There is informed consent for procedures, consent to be photographed and consent authorizing a disclosure.

- Documents providing written permission authorizing disclosure for a specific purpose:
 - Privacy Act – Consent
 - 38 USC 7332 – Special Consent
 - HIPAA Privacy Rule – Authorization
 - VHA Handbook 1605.1 – Authorization

For purposes of this training, the term "authorization" is used when discussing permission authorizing a disclosure instead of the word "consent."

REQUEST FOR AND AUTHORIZATION TO RELEASE MEDICAL RECORDS OR HEALTH INFORMATION

of this form does not authorize the release of information other than that specifically described below. The information disclosed in accordance with the Health Insurance Portability and Accountability Act, 45 CFR 164.512(a) is not furnished completely and accurately, Department of Veterans Affairs will be unable to process your application for treatment, payment, enrollment or eligibility on signing the authorization. VA may disclose the information to other VA systems of records notices identified as 24VA19 "Patient Information to identify veterans and persons claiming or receiving VA benefits and their records, and for other purposes. You do not have to provide the information to VA, but if you don't, VA will be unable to process your application for treatment, payment, enrollment or eligibility on signing the authorization. If you provide VA your Social Security Number, you are not required to respond to, a collection of information unless it displays a valid OMB number. This includes the time it will take to read instructions, gather the

I. SECURITY NUMBER IF THE PATIENT DATA CARD IMPRINT IS NOT USED.

4th	PATIENT NAME (Last, First, Middle Initial)
	[Redacted]
	SOCIAL SECURITY NUMBER
	[Redacted]
II. TO WHOM INFORMATION IS TO BE RELEASED	
[Redacted]	

Authorization Requirements, Part 1 of 2

If VHA employees receive a request for PHI that is accompanied by a valid written authorization, disclosure should be made in accordance with the authorization. When a valid written request, signed by the individual is made, every attempt to provide the disclosure should be made, unless the information requested is deemed **sensitive**. For additional information on sensitive information requests, contact your VHA health care facility Privacy Officer.

A written authorization is a document signed by the individual to whom the information or record pertains and may be required for use or disclosure of protected health information.

When a written authorization of the individual is required for use or disclosure of PHI, the authorization must contain each of the following elements to be valid:

- Be in writing,
- Identify the individual to whom the requested information pertains to,
- Identify the permitted recipient or user,
- Describe the information requested,
- Describe the purpose of the requested use or disclosure,
- Contain the signature of the individual whose records will be used or disclosed,
- Contain an expiration date, satisfaction of the need or an event,
- Include a statement that the patient may revoke the authorization in writing, except to the extent the facility has already reacted on it, and to whom the revocation is provided to,
- Include a statement that treatment, payment, enrollment, or eligibility for benefits cannot be conditioned on the individual completing an authorization,
- Include a statement that the information may no longer be protected from re-disclosure.

There are some cases when a written authorization is not required such as when:

- PHI is used for treatment, payment, and/or health care operations (TPO), or
- Other legal authority exists.

Authorization Requirements, Part 2 of 2

Authorization may be given on VA Form 10-5345, *Request for and Authorization to Release Medical Records or Health Information*.

VA Form 10-5345 is used to permit disclosures to third party requestors who are not the subject of the health information that is to be disclosed. VA Form 10-5345 can be initiated by the Veteran or a third party but it **must always** be signed by the subject of the record.

If any of the authorization requirements listed above, with exception to the Veteran request field (the specific authority to release 38 U.S.C. 7332 information) on the VA Form 10-5345, have not been satisfied the authorization will be considered invalid. If any of the following statements about the authorization are true, the authorization becomes invalid:

- Fails to meet all of the content requirements (See VA Form 10-5345).
- Expiration date on the VA Form 10-5345 has passed.
- Is known to have been revoked.
- Is known to be false with respect to the authorization requirements.



NOTE:

Unless it is explicitly covered in the authorization, information regarding testing or treatment of HIV or sickle cell anemia, or the treatment of or referral for drug/alcohol treatment must not be disclosed to a third party per 38 U.S.C. 7332.



NOTE:

A Veteran who is requesting his/her own health information is not required to submit an authorization, just a written request that is signed, dated and outlines the information being requested. A written request may be given on VA Form 10-5345a, *Individuals' Request for a Copy of Their Own Health Information*, or a hand written request (e.g., letter) signed by the individual.

Process a Request

Individuals or third parties may request VHA to disclose any record maintained by the Agency. The following describes how a request will be processed:

The request must be in writing and describe the record sought so it may be located in a reasonable amount of time. The majority of written requests are handled through the facility's Release of Information office.

If the requestor is the individual to whom the record pertains (first party), the individual has a first party right of access to receive a copy unless there is an exception, such as VA police records.

If the requestor is other than the individual to whom the record pertains (third party), determine what information or record is requested and that you have a valid written authorization from the individual or other legal authority to disclose the information.

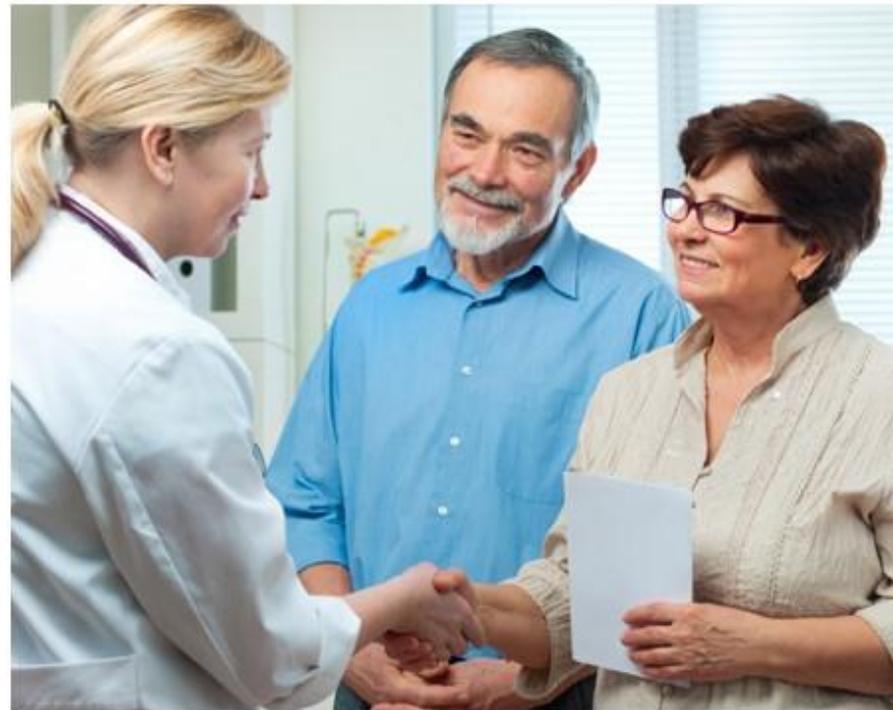
If the record requested does not fall under a Privacy Act System of Records (records that are retrieved by an individual's name or a unique identifier), the request must be processed in accordance with the Freedom of Information Act (FOIA) policy. If the request is considered a FOIA request, contact your facility's FOIA Officer to process the request.

VHA employees should process requests for PHI within the required time frame (i.e., 20 work days from receipt) and charge any applicable fees as outlined in VHA Handbook 1605.1.



NOTE:

If there are questions from VHA employees on legal authority to make disclosures, the VHA health care facility Privacy Officer should be contacted prior to making the disclosure.



Other Disclosures Requiring Authorization, Part 1 of 2

VHA has several policies for the disclosure of PHI for certain purposes. Discussed below is the VHA disclosure policy for the release of information for billing purposes that include 38 U.S.C 7332 protected information, requesting VBA claims folders, providing medical opinions, releasing of psychotherapy notes and taking video, photography or voice recordings.

BILLING OF INSURANCE CLAIMS: Billing staff may be requested to provide health information in support of an insurance claim. If upon review of the health information that is being requested there is 38 U.S.C 7332-protected information, such as Sickle Cell Anemia, treatment or referral for alcohol or drug abuse, or the testing or treatment for HIV, an authorization *must be* obtained prior to disclosing this information to the insurance company. Consult your VHA health care facility Privacy Officer for additional guidance and a process for obtaining the authorization.

MEDICAL OPINIONS: VHA health care providers are required, when requested, to provide descriptive statements and opinions for VHA patients with respect to the Veteran's medical condition, employability, and degree of disability. A copy of this opinion should be placed within their health record. A written request or authorization is to be obtained prior to the disclosure.

PSYCHOTHERAPY NOTES: Psychotherapy notes are created to carry out treatment; used to train students or participants in mental health programs; and in defense of a legal action. VHA employees may not disclose psychotherapy notes for any other purpose without the prior written authorization of the individual to whom the notes pertain. **Psychotherapy notes are personal notes maintained by the psychotherapist which are kept separate from documentation placed within the patient's health record in CPRS.** By definition, psychotherapy notes CANNOT be in the health record; therefore, any notes or information placed in a mental health progress note in CPRS are NOT psychotherapy notes.



NOTE:

Answers to psychological tests, i.e., Minnesota Multiphasic Personality Inventory (MMPI), Wechsler Adult Intelligence Scale (WAIS), etc., are considered forms used by VHA where an individual cannot seek access to the blank or completed tool, which is copyright protected. The individual may receive a copy of the final or summary assessment report.



NOTE:

An individual does not have a "right of access" to these psychotherapy notes. For additional information, contact your VHA health care facility Privacy Officer.

Department of Veterans Affairs		REQUEST FOR AND AUTHORIZATION TO RELEASE MEDICAL RECORDS OR HEALTH INFORMATION	
<small>Privacy Act and Paperwork Reduction Act Information: The execution of this form does not authorize the release of information other than that specifically described below. The information requested on this form is released under Title 38, U.S.C. The form authorizes release of information in accordance with the Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164, 5 U.S.C. 552a, and 38 U.S.C. 5701 and 7332 that you specify. Your disclosure of the information requested on this form is voluntary. However, if the information including Social Security Number (SSN) (the SSN will be used to locate records for release) is not furnished completely and accurately, Department of Veterans Affairs will be unable to comply with the request. The Veterans Health Administration may not condition treatment, payment, enrollment or eligibility on signing the authorization. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act system of records action identified as 26VLA19 "Veterans Medical Record - VA" and in accordance with the VHA Notice of Privacy Practices. You do not have to provide the information to VA, but if you don't, VA will be unable to process your request and save your medical records. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law. The Paperwork Reduction Act of 1995 requires us to notify you that this information collection is in accordance with the clearance requirements of section 5037 of the Paperwork Reduction Act of 1995. We may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB number. We anticipate that the time expended by all individuals who must complete this form will average 2 minutes. This includes the time it will take to read instructions, gather the necessary facts and fill out the form.</small>			
ENTER BELOW THE PATIENT'S NAME AND SOCIAL SECURITY NUMBER IF THE PATIENT DATA CARD IMPRINT IS NOT USED.			
<small>TO: DEPARTMENT OF VETERANS AFFAIRS (Print or type name and address of health care facility)</small>		<small>PATIENT NAME (Last, First, Middle Initial)</small>	
<div style="border: 1px solid black; padding: 2px;"> PLEASE RETURN CD(S) TO THE RELEASE OF INFORMATION OFFICE WHEN FINISHED! </div>		<div style="border: 1px solid black; padding: 2px;"> PATIENT NAME <small>SOCIAL SECURITY NUMBER</small> LAST FOUR </div>	
<small>NAME AND ADDRESS OF ORGANIZATION, INDIVIDUAL, OR TITLE OF INDIVIDUAL TO WHOM INFORMATION IS TO BE RELEASED</small>			
<div style="border: 1px solid black; padding: 2px;"> DOCTOR'S NAME AND PAGER # </div>			
<small>VETERAN'S REQUEST: I request and authorize Department of Veterans Affairs to release the information specified below to the organization, or individual named on this request. I understand that the information to be released includes information regarding the following condition(s):</small>			
<small> <input type="checkbox"/> DRUG ABUSE <input type="checkbox"/> ALCOHOLISM OR ALCOHOL ABUSE <input type="checkbox"/> TESTING FOR OR INFECTION WITH HUMAN IMMUNODEFICIENCY VIRUS (HIV) <input type="checkbox"/> SICKLE CELL ANEMIA INFORMATION REQUESTED (Check applicable box(es) and state the extent or nature of the information to be disclosed, giving the dates or approximate dates covered by each) </small>			
<small> <input type="checkbox"/> COPY OF HOSPITAL SUMMARY <input type="checkbox"/> COPY OF OUTPATIENT TREATMENT NOTES <input type="checkbox"/> OTHER (Specify) </small>			
<div style="border: 1px solid black; padding: 2px;"> THE INFORMATION YOU NEED INCLUDING DATES . . . </div>			

Other Disclosures Requiring Authorization, Part 2 of 2

TAKING VIDEO, PHOTOGRAPHS OR VOICE RECORDINGS: In order for video, voice/audio recordings or photographs to be taken for non-treatment purposes, there must be a local facility policy in place. A VHA employee wishing to take a patient's photograph or make a video or voice/audio recording for a purpose unrelated to the patient's health care, such as supporting continuing education efforts or a presentation at a conference, must get an authorization from the patient by having the patient sign VAF 10-3203, *Consent for Use of Picture and/or Voice*.



NOTE:

For research protocols, the IRB cannot waive the requirement for VAF 10-3203.

If the video, photograph or voice recording is going to be further disclosed then the patient must also sign VA Form 10-345, *Request for and Authorization to Release Medical Records or Health Information*, prior to making the disclosure.

The local facility policy should state that cell phones may be used in non-patient care areas such as lobbies, public waiting rooms, offices and cafeteria. Cell phones may be used in patient care areas, unless otherwise prohibited. Signage stating policy should be clearly posted in patient care areas, i.e. telemetry or ICU.

Cell phones with camera capability should only be used for phone calls. To ensure and protect the privacy of others, the camera feature may not be used anywhere on Federal property unless there is a policy that states otherwise. Facility signage at each entrance should clearly state whether photography is prohibited.

Employees or Non VA individuals are prohibited from secretly taking pictures, audio or video taping of each other.



Summary - Module 4

Congratulations! You have completed Module 4.

In this module you learned about

- Consent versus authorization
- When written authorization is necessary for disclosure of information
- Processing a request
- Managing disclosures and releases requiring authorization
- Taking video, photographs and voice recordings

In the next module, Release of Information Outside Of VA, you will learn what information can be disclosed to non-VA entities.

Specifically you will learn:

- Information that can be disclosed to non-VA entities such as Congress, courts of law, law enforcement, family members, non-VA health care providers, other federal agencies, public health authorities, State Veterans Homes, and Veteran Service Organizations (VSO)

Information that can be disclosed to a non-VA organization or entity.



Module 5 - Release of Information Outside of VA

Module 5 Introduction

In this module, you will learn what information can be disclosed to non-VA entities.

Specifically you will learn:

- Information that can be disclosed to non-VA entities such as Congress, courts of law, law enforcement, family members, non-VA health care providers, other federal agencies, public health authorities, state veterans homes, and Veteran Service Organizations (VSO).



Individual Authorization

Before making a disclosure of any protected health information to an outside entity without an individual's authorization, VHA employees should determine:

- The type of information involved, and
- Whether legal authority exists under the statutes and regulations to permit the disclosure.

If legal authority is not found in **all** six applicable statutes and regulations (as discussed in Module 1), VHA employees may not make the disclosure.

Disclosure is not mandatory under these provisions. In situations where it is unclear whether legal authority exists, the signed authorization of the individual should be obtained.

An accounting of disclosures is required for all disclosures discussed in this module.



Non-VA Entities



Information can be disclosed to various non-VA entities:

- Congress
- Courts
- Law Enforcement
- Next of Kin, Family and Significant Others
- Non-VA Health Care Providers
- Non-VA Health Care Referral to VHA
- Emergency Non-VA Health Care
- Organ Procurement Organizations (OPO)
- Public Health Authorities
- State Veterans Homes
- Veterans Service Organizations (VSO)

Congress

VHA may disclose protected health information to a member of Congress when responding to an inquiry from a congressional office that is made at the request of the individual to whom the information pertains. If a prior signed written authorization form has not been provided, the member of Congress needs to provide a copy of the original correspondence from the individual.

Protected health information may be disclosed to a congressional oversight committee or sub-committee without the individual's signed written authorization provided the request is made in writing, signed by the committee Chair, and on official letterhead.



NOTE:

For specific requirements related to congressional oversight inquiries, please contact your local health care facility Privacy Officer.

VHA employees may not disclose PHI upon an inquiry from a member of Congress on behalf of the Veteran by a third party (e.g., Veteran's son) without an appropriate signed written authorization.



Courts

Courts

VHA employees may disclose PHI pursuant to a **court order** from a Federal, State, or local court of **competent jurisdiction**. Refer to VHA Handbook 1605.1, *Privacy and Release of Information* for further guidance.

A **subpoena** is not sufficient authority to disclose PHI unless the subpoena is signed by the judge of a court of competent jurisdiction or it is accompanied by the written authorization of the individual whose records are the subject of the subpoena.

If there is 38 USC 7332 information that is being requested then a very specific court order will be required.



NOTE:

All court orders or subpoenas should be referred to the health care facility Privacy Officer for coordination with their local Regional Counsel prior to disclosure of health information or VHA employee appearance.

Competency Hearings

VHA may disclose PHI to private attorneys representing Veterans deemed **incompetent** or declared incapacitated for a competency hearing when a court order, discovery request or other lawful process is provided, as long as the individual has been given notice of the request.

There is no authority to disclose information directly to the Veteran's Next of Kin unless the Next of Kin is a personal representative of the individual. A court order is required.



Routine Reporting to Law Enforcement Entities Pursuant to Standing Written Request Letters

Protected health information, **EXCLUDING 38 U.S.C. 7332-protected information**, may be disclosed to officials of any criminal or civil law enforcement governmental agency charged under applicable law with the protection of public health or safety in response to a standing written request letter.

Protected health information may be disclosed to a Parole Officer with a signed written authorization from the individual.

Child, adult, and elder abuse requires a standing written request letter prior to reporting to a law enforcement agency unless abuse is serious and imminent to the health and safety of the individual.



NOTES:

Prior to disclosure to a law enforcement agency, please check with your local health care Privacy Officer as to whether a valid standing request letter is on file. The standing written request letter must be updated in writing every 3 years.



Next of Kin, Family and Significant Others

General information on the patient's condition and location can be discussed with the general public if the patient has not opted out of the facility directory.

Protected health information can be shared in the presence of others as long as the patient does not object

Protected health information can be shared outside the presence of the patient when, in the professional judgment of the provider, it is determined the disclosure is in the best interest of the patient

HIV Status may be disclosed by a clinical practitioner to the patient's spouse or sexual partner if certain conditions are met, such as the HIV positive patient does not intend to tell his/her spouse or sexual partner of his/her status.



Non-VA Health Care Provider and Referral

Non-VA Health Care Provider

VHA may disclose PHI, **excluding 38 U.S.C. 7332 protected information**, to a non-VA health care provider for the purposes of VA paying for services without a signed written authorization.

VHA may disclose PHI, **excluding 38 U.S.C. 7332 protected information**, to a non-VA health care provider for the purposes of treatment without a signed written authorization.

VHA may disclose any PHI to medical personnel to the extent necessary to meet a bona fide medical emergency including 38 U.S.C. 7332 protected information.



NOTE:

The minimum necessary standard does not apply to treatment purposes.

Non-VA Health Care Referral

For the purpose of health care referrals, VHA may disclose PHI; excluding 38 U.S.C. 7332 protected health information, to resident care homes, assisted living facilities, and home health services. Providers such as social workers cannot disclose that the Veteran has 38 USC 7332 protected diagnoses without an authorization from the Veteran.



Organ Procurement Organization

As long as VHA Handbook 1101.03, *Organ, Tissue, and Eye Donation Process* is followed, VHA may disclose relevant health information for the purpose of determining suitability of a patient's organs or tissues for organ donation to an Organ Procurement Organization (OPO) without authorization if all of the four following conditions are met

- Individual is an inpatient in a VA health care facility
- Individual is near-death or deceased
- VHA has a signed agreement with the OPO
- OPO is certified with Health and Human Services

Contact the facility OPO Coordinator for additional stipulations prior to making a disclosure.



Public Health Authorities

VHA employees may disclose protected health information, excluding 38 U.S.C. 7332 protected information, to Federal, State, and/or local public health authorities charged with the protection of the public health or safety pursuant to a standing written request letter or other applicable legal authority. A standing written request letter is good for a period of three years. After that period of time, the letter must be re-issued.

An individual's infection with HIV may be disclosed from a record to a Federal, State, or local public health authority that is charged under Federal or State law with the protection of the public pursuant to a standing written request letter. An authorization is not required for this disclosure. Please refer to your VHA health care facility Privacy Officer for additional guidance.

Influenza ("Flu") vaccination or illness reporting is only allowed if required by state law and covered under a standing written request letter.



State Veterans Homes

VHA employees may disclose protected health information, excluding 38 U.S.C. 7332 protected information, to Federal, State, and/or local public health authorities charged with the protection of the public health or safety pursuant to a standing written request letter or other applicable legal authority. A standing written request letter is good for a period of three years. After that period of time, the letter must be re-issued.

An individual's infection with HIV may be disclosed from a record to a Federal, State, or local public health authority that is charged under Federal or State law with the protection of the public pursuant to a standing written request letter. An authorization is not required for this disclosure. Please refer to your VHA health care facility Privacy Officer for additional guidance.

Influenza ("Flu") vaccination or illness reporting is only allowed if required by state law and covered under a standing written request letter.



Veteran Service Organizations (VSO)

VHA employees may disclose protected health information to a Veterans Service Organization for purposes of obtaining benefits provided an appropriate *Power of Attorney* (POA) or a signed written authorization from the individual has been filed with the VA health care facility that maintains the information.

For additional information on VSO's requesting access to the electronic health record, refer to the following website at <http://vawww.va.gov/hia/UserGroups.htm>.



Summary - Module 5

Congratulations! You have completed Module 5.

In this module you learned about

- Disclosure procedures to non-VA entities.

In the next module, Operational Privacy Requirements, you will learn general requirements for agency accounting of disclosures, complaints, faxes, emails, health information from non-VA physicians and facilities, contracting and training.



Module 6 - Operational Privacy Requirements

In this module, you will learn the general requirements for operational management when releasing individually identifiable information.

Specifically you will learn:

- General requirements for privacy management during accounting of disclosures, complaints, faxes, emails, health information from non-VA physicians and facilities, training of employees, delegation of a Privacy Officer, contracts and penalties
- Virtual lifetime electronic Record (VLER)

At the end of this module, you will be able to identify the general requirements for operational management to ensure privacy when releasing Veteran information.



Complaints

Individuals have the right to file a complaint regarding VHA privacy practices. The complaint does not have to be in writing, though it is recommended.

All complaints, **regardless of validity**, must be entered into Privacy and Security Event Tracking System (PSETS) within one hour of discovery during normal business hours or as soon as possible outside of normal business hours.



Faxes

VHA health care facilities should only transmit PHI via facsimile (fax) when no other means exists to provide the required information in a reasonable manner or time frame.

VHA health care facilities need to ensure PHI is sent on a machine that is in secure locations and not accessible to the general public.

VHA health care facilities shall take reasonable steps to ensure the fax transmission is sent to the appropriate destination (e.g. call the requestor to ensure receipt). A confidentiality statement must be on the cover page when transmitting PHI. The statement will instruct the recipient of the transmission and to notify VHA if received in error.



Email

Email messages must contain only non-PHI unless the data is encrypted (i.e., PKI or RMS). Contact your facility Information Security Officer and VA Handbook 6500, *Information Security Program*, and VA Directive 6301, *Electronic Mail Records*, for additional guidance.

Microsoft Outlook calendars and Microsoft Communicator are not to be used to store Veteran's PHI.

Vista Email can be used to share PHI internally; however the Veterans name or other identifiers should not be placed in the subject line of the message.

Provider-to-patient emails are prohibited if they include PHI. Use secure messaging in MyHealthVet for those communications that include PHI.



NOTE:

Veterans cannot give permission to communicate with them via email as it is against VA policy.



Penalties

Individuals who are convicted of knowingly and willfully violating the penalty provisions of the Privacy Act shall be guilty of a misdemeanor and fined not more than \$5,000.

In the event a health care facility employee is found criminally liable of a privacy violation, a written report of the incident will be provided to the VHA health care facility Director.

Any person who violates any provision of 38 U.S.C. 7332 shall be fined not more than \$5,000 in the case of a first offense, and not more than \$20,000 in each subsequent offense. A VHA employee who knowingly violates the provisions of *Health Insurance Portability and Accountability Act (HIPAA)* and the *American Recovery and Reinvestment Act of 2009 (ARRA)*, by disclosing PHI shall be fined not more than \$50,000, imprisoned not more than one year, or both. Offenses committed under false pretenses or with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm have more stringent penalties.

In addition to the statutory penalties for the violations described above, administrative, disciplinary, or other adverse actions (e.g., admonishment, reprimand, and/or termination) may be taken against employees who violate the statutory provisions.



Training of Personnel

All VHA personnel including employees, volunteers, contractors and students must be trained, at least annually, on privacy policies to include the requirements of Federal privacy and information laws, regulations, HIPAA and VHA policy. New personnel must be trained within 30 days of employment or sooner if required for computer access. This training must be completed **prior** to the new personnel being allowed access to PHI.

At a minimum, instruction must be provided within 6 months of any significant change in Federal law, regulation, this policy, and/or facility or office procedures. VHA health care facilities must track completion of privacy training and be prepared to report privacy training completion figures.

In VHA all privacy training is done on an annual anniversary date of when the training was taken the previous year. All required training must be done in the Talent Management Service (TMS) system. This will ensure that the training is appropriately documented for tracking purposes.



Designation of Privacy Officer

Each administration must designate at least one facility Privacy Officer. VISN and VA Medical Centers (VAMC) or Health Care Systems (HCS) may designate more than one full-time VHA health care facility Privacy Officer if the size and complexity of the facility warrant the need. Many HCSs or VAMCs may have the FOIA Officer and the VHA health care facility Privacy Officer as the same person.



NOTE:

It is the employee's responsibility to know the name of their assigned health care facility Privacy Officer or Administration Privacy Officer.

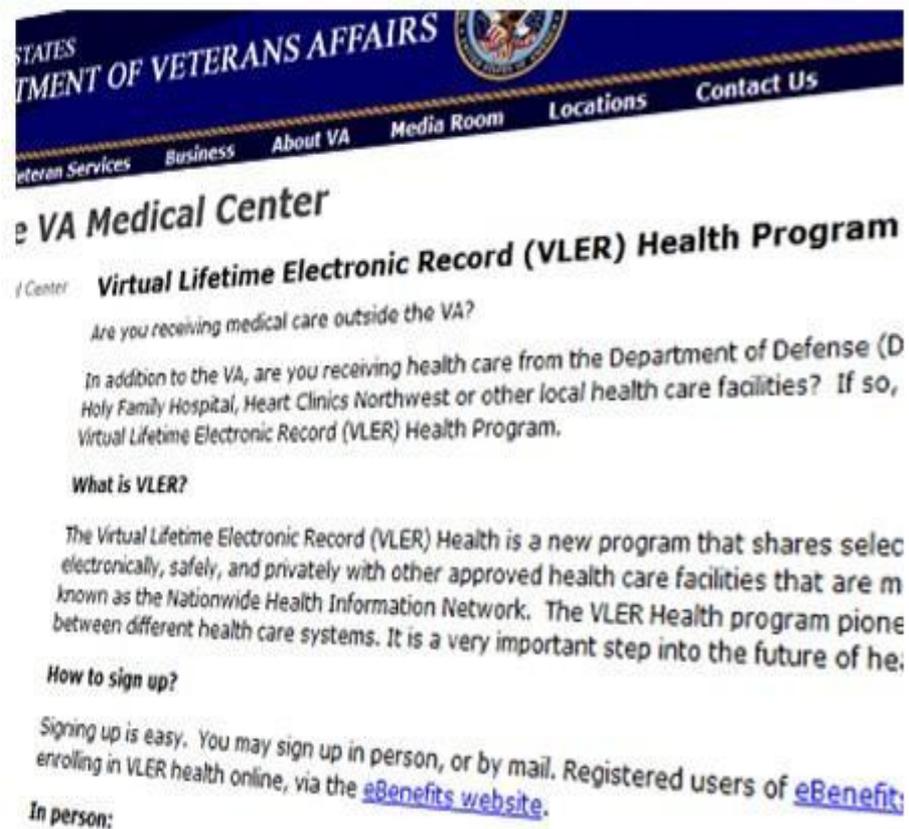


Virtual Lifetime Electronic Record

In April 2009, President Obama directed the VA and DoD to lead the efforts in creating VLER (Virtual Lifetime Electronic Record), which would "ultimately contain administrative and medical information from the day an individual enters military service throughout their military career and after they leave the military."

VLER utilizes the Nationwide Health Information Network (NwHIN) to share prescribed patient information via this protected network environment with participating private health care providers, but this does not involve 'scanned' patient information.

The participating providers will have a 'view only' option to see the Veteran's information once the Veteran has completed an authorization (VA Form 10-0485). Once a patient completes all forms required, the patient is then "opted-in" for sharing of their health information.



The screenshot shows the top navigation bar of the VA website with the following links: [Veteran Services](#), [Business](#), [About VA](#), [Media Room](#), [Locations](#), and [Contact Us](#). The main heading is **e VA Medical Center**. Below it is the title **Virtual Lifetime Electronic Record (VLER) Health Program**. The content includes a question: "Are you receiving medical care outside the VA?" followed by a paragraph: "In addition to the VA, are you receiving health care from the Department of Defense (D Holy Family Hospital, Heart Clinics Northwest or other local health care facilities? If so, Virtual Lifetime Electronic Record (VLER) Health Program." Below this is the section **What is VLER?** with the text: "The Virtual Lifetime Electronic Record (VLER) Health is a new program that shares selected electronically, safely, and privately with other approved health care facilities that are known as the Nationwide Health Information Network. The VLER Health program pions between different health care systems. It is a very important step into the future of he." The next section is **How to sign up?** with the text: "Signing up is easy. You may sign up in person, or by mail. Registered users of [eBenefits](#) enrolling in VLER health online, via the [eBenefits website](#)." The final section is **In person:**.

Summary - Module 6

Congratulations! You have completed Module 6.

In this module you learned about the requirements:

- For operational management and ensuring privacy when releasing information
- VLER

In the next module, Module 7, you will learn about the Freedom of Information Act (FOIA).



Module 7 - Freedom of Information Act (FOIA)

In this module you will learn about the elements of the Freedom of Information Act (FOIA). Specifically, you will learn about

- Elements of the FOIA
- Access
- Employee Responsibilities
- Who Can Make A FOIA Request
- Procedural Steps
- Agency Records
- Time limits for a FOIA Request
- Consequences of Untimely Responses
- Exemptions
- Litigation
- The Annual Report of Compliance

At the end of this module, you will be able to identify the elements of the Freedom of Information Act (FOIA).



Elements of FOIA

Elements of FOIA:

- Enacted by Congress in 1966
- Effective: July 5th, 1967
- The basic purpose of the FOIA is "to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold governors accountable to the governed."
- The FOIA establishes a presumption that records in the possession of agencies and departments of the executive branch of the U.S. Government are accessible to the people.
- FOIA is concerned with affording the most **disclosure** of information under law.
- The FOIA sets standards for determining which records must be disclosed and which records may be withheld.
- The law also provides administrative and judicial remedies for those denied access to records.



Access

The FOIA requires disclosure of records, in the possession of VA, upon the written request of an individual or organization.

Written requests may be received by mail, by hand, by email or fax. Requests made under the FOIA must reasonably describe the records being requested. If VHA employees receive written FOIA requests for records, such requests should be forwarded to the local FOIA Officer.

The FOIA Officer will make all determinations regarding release of the requested records.

Records that have been destroyed as part of the VA's approved records retention schedule are not subject to FOIA. However, any records not destroyed in accordance with the approved records retention schedule must be provided in response to the FOIA request.



Employee Responsibilities

Employee Responsibilities

- All employees are required to fully cooperate in the handling of FOIA requests as directed by the local FOIA Officer.
- Specific employee responsibilities include:
 - Searching for agency records at the direction of the local FOIA Officer
 - Fully documenting the FOIA search efforts to include time spent searching, search terms utilized, and identification of systems or files searched
 - Providing responsive records to the FOIA Officer in a timely manner, this includes providing records in the format requested by the requestor, if available.
 - Being accessible to the FOIA Officer for questions/clarifications
 - Fee estimates at the direction of the FOIA Officer

Employees should not contact a FOIA requestor. All communications with a FOIA requestor must be made by the FOIA Officer.



Who Can Make a FOIA Request?

- Virtually ANYONE, including:
 - Private citizens
 - Members of Congress
 - Corporations, associations, partnerships
 - Foreign and domestic governments
 - Unions
 - Other federal employees, except when made in the official performance of their VA duties

- Exceptions:
 - Federal agencies may not use the FOIA as a means of obtaining information from other federal agencies
 - Congressional oversight committees may not be denied information on the basis of a FOIA exemption
 - Fugitives from justice, when the requested records relate to the requestor's fugitive status

Procedural Request

Once you receive a FOIA request, you should promptly refer it to your facility or administration FOIA Officer. You may find the appropriate FOIA Officer using the FOIA Officer Contact roster on the VA FOIA Homepage at <http://www.foia.va.gov/>.

- Once the facility or administration FOIA Officer has issued the records search assignment, the VHA health care facility or program office with the records in question should promptly provide copies of the records to the facility or administration FOIA Officer in accordance with the time frame set by the FOIA Officer.

DEPARTMENT OF VETERANS AFFAIRS

Home Veteran Services Business About VA Media Room Locations

Quick Links

- [FOIA Home Page](#)
- [How to submit a FOIA request](#)
- [Where to submit a FOIA request](#)
- [Fee Information](#)
- [How to appeal a FOIA request](#)
- [FOIA Reading Room](#)

Freedom of Information Act

The Freedom of Information Act (FOIA) provides the right of access to Federal agency records, except records are protected from release by a FOIA enforcement record exclusion. It is VA's policy to the fullest extent under the law. The VA has a handling FOIA requests. All FOIA requests should be submitted to any of the approximately 400 geographic offices that maintain the records you are seeking.

VA Benefits Records

Submit your request to the FOIA/Private Office serving the individual's jurisdiction. For example, the FOIA/Private Office of the Veterans Benefits Administration (Compensation and Pension, Loan Guarantees, and E

Agency Records

What Agency Records Are...

- Either created or obtained by an agency; and
- Under agency control at the time of the FOIA request

Four factors for determining if an agency has "control" of the records:

- The intent of the record's creator to retain or relinquish control over the record;
- The ability of the agency to use and dispose of the record as it sees fit;
- The extent to which agency personnel have read or relied upon the record; and,
- The degree to which the record was integrated into the agency's records systems or files.



Time Limits for a FOIA Request

A request for records received will be promptly referred for action to the appropriate VA FOIA Officer. The requestor must be notified in writing within 20 work days after receipt of the request whether the request will be granted or denied. If granted in whole or in part, copies of the records being requested must be provided within this statutory timeframe.

An agency may extend the 20 work day time limit to process a FOIA request an extra 10 work days under "unusual circumstances" as determined by the FOIA Officer. The FOIA Officer must notify the FOIA requestor in writing of this extension before the 20 work day time limit passes.



Consequences of Failure to Process Requests Timely

- If the agency fails to meet these time limits for initial processing of a FOIA request, the FOIA requestor may file a lawsuit seeking the records.
- Failure to process a FOIA request timely can result in several adverse consequences for the agency. These include:
 - Limitations on the fees that the facility may charge the requestor;
 - Adverse publicity for the facility, including allegations of improper motives for the delay in processing.
 - The requestor may be able to immediately file suit seeking the records, and Section 4 of the Open Government Act allows for the payment of attorney fees and other litigation costs to be paid to FOIA plaintiff(s) when they prevail in the lawsuit.



Exemptions from Public Access to VA Records

There are nine exemptions that permit withholding of certain information from disclosure. It is the general policy of VA to disclose information from Department records to the maximum extent permitted by law. There are circumstances, however, when a record should not or cannot be disclosed in response to a FOIA request. When such an occasion arises, the FOIA permits records or information, or portions that may be segregated to be withheld under one or more of the exemptions.

Determinations as to whether a FOIA exemption is applicable to certain records are made solely by the FOIA Officer. When withholding information pursuant to one of the nine exemptions, the agency must provide the requestor with certain specific information about the action taken on the request, including an estimate of the amount of denied information, unless doing so would undermine the protection provided by the exemption.

Types of agency records that may be exempt and withheld from release under a FOIA exemption:

- Exemption 1 – National Defense or Classified Records
- Exemption 2 – Internal Personnel Rules and Practices
- Exemption 3 – Records Exempted by Another Law or Statute
- Exemption 4 – Commercial Financial and Trade Secrets
- Exemption 5 – Inter- and Intra-Agency Documents
- Exemption 6 – Records Containing Information that Invades the Personal Privacy of an Individual
- Exemption 7 – Law Enforcement Records
- Exemption 8 – Financial Institutions Records
- Exemption 9 – Geological and Geophysical Records



EXEMPTIONS

Litigation

- If a FOIA request is litigated, the FOIA Officer will be notified by the VA OGC.
- The VA OGC serves as the liaison for the VA to the Department of Justice, Assistant U.S. Attorney who handles the litigation.
- All VA employees are expected to timely comply with the guidance and direction provided by the FOIA Officer and the VA OGC in the course of representing VA in a FOIA lawsuit.



Annual Report of Compliance

The FOIA requires each agency to submit to Congress a report on or before March 1st of each year of its activities and efforts to administer the FOIA during the preceding fiscal year. The facility FOIA Officer is required to submit figures referencing FOIA requests annually to VA Central Office (VACO).



Summary - Module 7

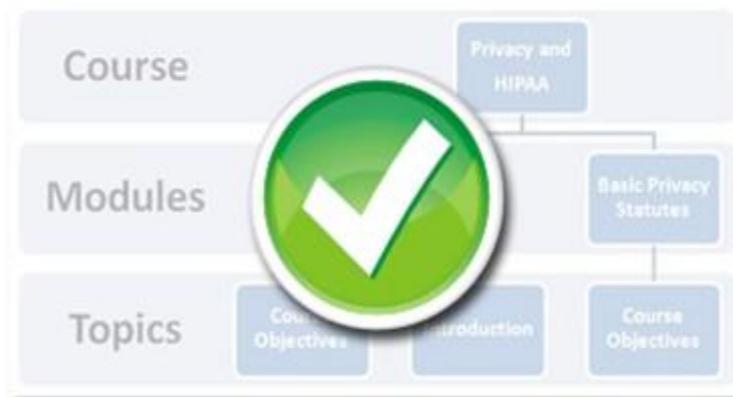
Congratulations! You have completed Module 7.

In this module, you learned about the elements of the Freedom of Information Act (FOIA)

- Elements of the FOIA
- Access
- Employee Responsibilities
- Who Can Make A FOIA Request
- Procedural Steps
- Agency Records
- Time limits for a FOIA Request
- Consequences of Untimely Responses
- Exemptions
- Litigation
- The Annual Report of Compliance

Congratulations! You have completed all seven modules. Please go to module eight to:

- Get a copy of the text or power point version of this training
- Print your completion of the training certificate
- Receive the number to the help desk



Module 8 - End of Course Instructions

During this course, you have learned about

- Basic Privacy Laws and Regulations
- Veterans Rights
- Uses and Disclosures of Information in VA
- Purposes that Require an Authorization
- Releases of Information Outside of VA
- Operational Privacy Requirements and
- Freedom of Information Act (FOIA)



Course Conclusion

This concludes the Privacy and HIPAA Training for FY2013.

For more information on Privacy and Release of Information, contact your VHA health care facility Privacy Officer or Administration Privacy Officer.

For a list of VHA Privacy Officers, go to <http://vawww.vhaco.va.gov/privacy/vhapo.htm>.

For a copy of the power point or text version of the training, please click <https://www.tms.va.gov>.

Thank you for your participation.



VHA Privacy and HIPAA Training FY2013

VOLUNTEER PRIVACY/HIPAA

Key Components

INTRODUCTION

Per VA regulations, all Regularly Scheduled volunteers are to have initial and annual privacy training. Given the various assignments of volunteers, a print version of the VHA Privacy and HIPAA Training is made available to volunteers. Volunteers who have computer access and who are issued a PIV badge must complete their privacy training through the TMS on-line education portal.

This document supplements the Privacy and HIPAA training packet, does not replace, listing key components of privacy and HIPAA practices related to volunteer assignments. A full copy of the 2013 Privacy and HIPAA Training document is available for review in the Voluntary Services Office, room 207-C, the Volunteer Escort Office, room 202-C, the Recreational Therapy Department and Chaplain Services. The document can also be viewed/downloaded from VA Butler's website, www.butler.va.gov.

As a VA Butler Healthcare volunteer, you are subject to the same expectations, rules and regulations as employees with respect to protecting the privacy, confidentiality and information security of the Veterans we serve and the staff and volunteers you serve with.

KEY COMPONENTS

- 1. PRIVACY OFFICER:** Each VA facility has a Privacy Officer who assists ensures that the facility has, and is in compliance with, privacy policies and procedures in place, to investigate breaches in privacy, to train staff, volunteers and Veterans on privacy procedures and to make rounds within the facility and the community clinics to look for privacy weaknesses. A mandatory poster is located on each floor/building at VA Butler Healthcare and the community clinics listing the contact information and photo of VA Butler's Privacy Officer. Volunteers may contact the privacy officer at any time to discuss any issues or concerns relative to privacy. The Privacy Officer for VA Butler Healthcare is as follows:
 - ***David Blackwell, Privacy Officer, 724-285-2416, VA Butler Healthcare, Bldg. 1, room 344W***
 - ***Sue Legacy, Backup Privacy Officer, 724-477-5066, VA Butler Healthcare, Bldg. 1, room 202E***

- 2. WHAT HAPPENS AT THE VA STAYS AT THE VA:** What you hear or see while providing volunteer services at VA Butler Healthcare is not to be discussed with individuals outside of the VA, discussed publicly within the VA or with others within the VA who do not have a right to that information. Any issues or concerns you have regarding a Veteran, staff person or other volunteer should be discussed with your immediate work site supervisor, the Privacy Officer or the Voluntary Services Coordinator in a secure, non-public area. Documents containing personal identifiable information on Veterans, staff or volunteers are not to be removed from the VA premises, emailed or faxed. There are certain exceptions, and those are/would be reviewed and authorized through the Privacy Officer.
- 3. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA):** The *Standards for Privacy of Individually Identifiable Health Information* (Privacy Rule) established, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Privacy Rule standards address the use and disclosure of individuals' health information (called "protected health information" by organizations subject to the Privacy Rule, called "covered entities"), as well as standards for individuals' privacy rights to understand and control how their health information is used. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the healthcare marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed. To view the entire Rule, go online to <http://www.hhs.gov/ocr/hipaa>. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996, with sections 261 through 264 of HIPAA requiring the Secretary of Health and Human Services to publicize standards for the electronic exchange, privacy and security of health information.
- 4. STATUTES THAT GOVERN THE COLLECTION, MAINTENANCE AND RELEASE OF INFORMATION FROM VETERANS HEALTH ADMINISTRATIVE RECORDS:** To review these statutes, you may conduct your own on-line search or you may contact the Privacy Officer.

- The Freedom of Information Act (FOIA), 5 U.S.C 552
- The Privacy Act (PA), 5 U.S.C. 552a
- Confidentiality Nature of Claims, 38 U.S.C, 5701
- Confidentiality of Certain Medical Records, 38 U.S.C. 7332
- Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. 5705
- The Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulation the HIPAA Privacy Rule.

5. RIGHT TO PRIVACY: Privacy is everyone’s right, especially our Veterans. Privacy strives to maintain balance between management of health information and protecting the Veteran’s privacy.

- Patients admitted as inpatients may **opt out** of the inpatient facility directory, and therefore, will not receive mail, calls or visitors. As a volunteer if you are asked if a patient is here, you are to refer the individual to the switchboard or to the nursing station. The switchboard and the nursing station maintain a list of those patients who have opted out of the inpatient directory.
- Veterans are provided a **Notice of Privacy Practices** informing them of how information may be used or disclosed by the VA, what the Veterans rights are regarding that information and the VA’s duties to protect that information. Copies of this notice may be obtained from the facility where the Veteran is receiving care or online at:
<http://www.1.va.gov/vhabpublications/viewpublication.asp?pub ID=1089>.
- The Community Living Center and the Domiciliary are considered “homes” to the patients who are admitted into these programs. As such, staff and volunteers are to respect the privacy of the Veteran and to “knock” on his/her door and to ask for permission to enter the patient’s room. Volunteers are not permitted into the rooms of patients in the Domiciliary. Unless advised to do so, Volunteers are not to enter patient’s rooms when the door is closed.

6. WHAT INFORMATION IS PROTECTED: Name, addresses, social security number, date of birth, diagnoses, admission to the hospital as an inpatient if requested by the patient, other medical and personal information. If you are not sure what information is protected, please contact your assignment site supervisor, the Privacy Officer or the Voluntary Services Coordinator.

- Volunteers are not permitted to take photographs of Veterans, staff and other volunteers at any time as that the taking of these photos is considered protected. *Photos may be taken with advanced authorization/clearance from the Public Affairs Officer.*

- 7. USE OF INFORMATION WITHIN THE VA:** Employees may use personal health identifiers on a need to know basis for their official job duties for purposes of treatment, payment and/or health care operations. The dissemination of patient information is governed by the rules and regulations as noted above and subject to strict policies and procedures to insure that the Veterans privacy is being maintained. To ensure compliance and understanding of the privacy regulations, employees are required to complete annual Privacy and HIPAA training, sign the Rules of Behavior and complete Information Security training. Electronic information may only be sent via protected communications (i.e. PKI). Faxes are to have cover sheets. These coversheets can be found on VA Butler's sharepoint site. Documents containing personal identifiable information are to be sent via privacy envelopes with the disclaimer letter attached. VA Butler volunteers, as part of their authorized assignment, may need to know some personal identifiers, such as name, address, last 4, and date of birth, in completion of an assignment. In this regard, the program for which the volunteer serves has/will provide on-site, on-going training that includes a review of the privacy and confidentiality controls for that program area and assignment.
- 8. PENALTIES:** Dependent upon the nature and severity of the breach, volunteers may be subject to the same criminal penalties as employees for breaches of privacy and security. Volunteers who do not adhere to the expectations and abide by the rules and regulations as set forth for the prevention and protection of an individuals privacy will be terminated from service at VA Butler Healthcare.
- 9. YOUR RESPONSIBILITIES AS A VOLUNTEER:** As a VA Butler Healthcare volunteer, your responsibilities are (but not limited to):
- Complete Privacy Training – initially and annually thereafter for the duration of your volunteer service
 - Know the particular requirements and parameters of your work site with respect to privacy and confidentiality
 - Through your actions, be a positive role model and an advocate for protecting the rights, privacy and confidentiality of the Veterans you serve and the staff and volunteers you work with
 - Double check your work and don't hurry – i.e., when doing mailings, check to make sure that the name on the letter matches the name on the envelope
 - Do not acknowledge that an inpatient is at this facility – refer face-to-face or telephone inquiries to the switchboard or the nursing stations of the Community

Living Center. These locations maintain a list of those inpatients who have opted out of the directory

- Do not discuss/share information/documents pertaining to Veterans, staff or other volunteers in public areas, outside the facility or internally with individuals who do not have a need to know
- Do discuss issues and concerns with appropriate program staff within secure environments
- Report actual privacy violation instances or possible instances. For example: If you see paperwork lying around the facility (i.e. waiting rooms, break rooms, etc.) that contain personal identifiable information, please take that information to the nearest employee, your site supervisor, the Voluntary Services Coordinator or Privacy Officer immediately. If you are opening mail for a department and the information contained within the envelope should have been sent via a privacy envelope, report the incident to your site supervisor.
- Do not use another person's PIV Badge to gain entrance to restricted areas.
- Do not document personal identifiable information nor make copies of documents that contain such information and take off site
- Protect your own privacy – be mindful of the information you discuss with others
- If you make a mistake, report it to your site supervisor immediately so that they can remedy the situation at that time or correct for the future
- Provide regular feedback

PRIVACY AND HIPAA TRAINING CERTIFICATE OF COMPLETION

I, _____ certify that I have completed
(print name)
the 2013 Privacy and HIPAA Training (print version) as required for
my volunteer service at VA Butler Healthcare. By completing this
training, I understand my role in protecting the privacy and
confidentiality of other individuals (Veterans, staff and volunteers) and
the governing rules and regulations. I also understand that there is zero
tolerance for breaches in privacy and that such behavior will/could result
in termination from the volunteer program.

I completed this training on _____
(date).

(signature of volunteer)

(signature of Voluntary Services Coordinator)