Department of Veterans Affairs

Employee Education System

and

VHA Office of Informatics and Analytics

Information Access and Privacy Office

Present

Privacy and HIPAA Training

Text Version FY 2012

October 1, 2011-September 30, 2012

Revised September 2011

Welcome

Welcome to the Privacy and HIPAA Training Web Site. This site will allow you take the mandatory training course detailing the Privacy and HIPAA training. This course is designed to be finished in 50-60 minutes.

Staff with access to VHA computer systems and/or access to protected health information (PHI) are required to complete this training annually on their anniversary date of which they took the training the previous year. All new employees who have access to VHA computer systems or have access to PHI are required to take this training within 30 days of hire. A team of subject matter experts from the VHA Privacy Office have created this training.

Course Overview

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA). Revisions have been made published 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.

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).

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

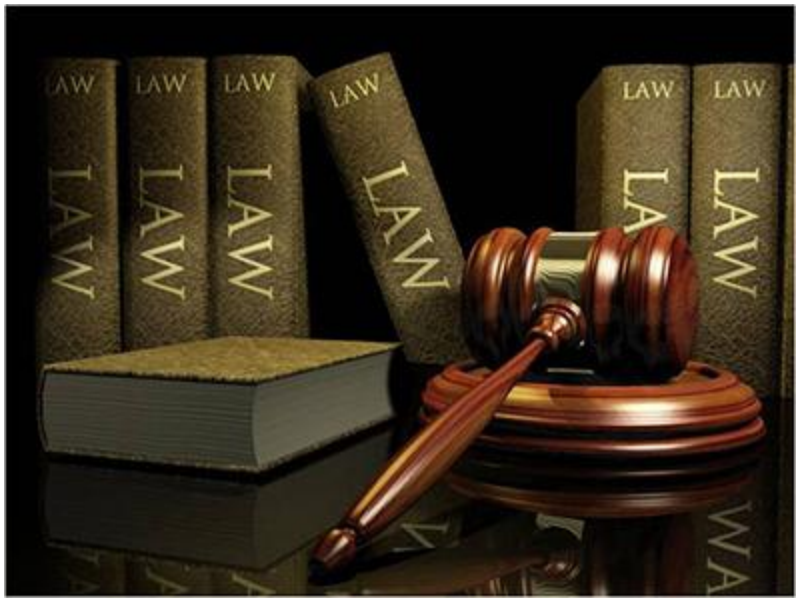
Course Objectives

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 and;
- Elements of the Freedom of Information Act (FOIA).

Note; Its is important that the privacy and HIPPA 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 requirement. For additional information on these topics contact your administration or VHA health care facility privacy officer.

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 regard 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 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/FOIA 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

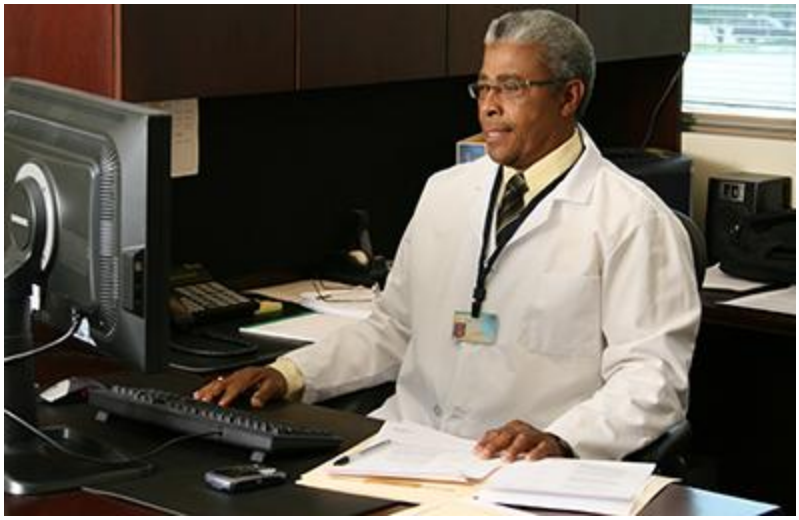
De-identified information is not considered to be individually identifiable; therefore, the provisions of the Privacy Act, HIPAA, and VA confidentiality statutes do not apply. VHA may disclose de-identified information under FOIA and must be processed by the FOIA Officer.

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-identied health information.

Use of Information



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

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.

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 – Administrative and Physical

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

Some administrative, physical and technical 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.
    - An example of this would be limiting the size of your Outlook mail.

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 to be 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).

Module 1 Summary

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

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)

NOTICE OF PRIVACY PRACTICES

Frequently Asked Questions

What are Privacy Practices?

Privacy practices are the ways in which the Department of Veterans Affairs (VA) and the Veterans Health Administration (VHA) manages, uses and shares your health information.

What is this *Notice of Privacy Practices* about?

The *Notice of Privacy Practices* defines health information and informs you of how this information may be used or disclosed by VHA, what your rights are regarding it, and what our duties are to protect it.

Why am I receiving this *Notice of Privacy Practices*?

The Health Insurance Portability and Accountability Act, better known as HIPAA, requires VHA to provide this Notice to all Veterans enrolled in health care benefits every three years. The Notice describes the privacy rights of a "patient". It

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.

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. Except for rare circumstances such as requiring a sensitive record review, Veterans may gain access to any information pertaining to them that is contained in any system of records.

Note: VA police records **do not** have a first party right of access provision.

All requests for copies will be delivered to, and reviewed by, the VHA health care facility Privacy Officer or designee. 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.

When an access request is withheld due to sensitive information, a letter must be sent to the Veteran. For additional information on withholding sensitive information, contact the VHA health care facility Privacy Officer. VHA health care facilities are to process all requests for review or copies of PHI within 20 work days of receipt whenever possible.

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.

If the Veteran requests an amendment of their health record, the VHA health care facility Privacy Officer will refer the request and related record to the health care provider or physician who is the **author** of the information to determine if the health record should be amended. When a request to amend a record is approved, the VHA health care facility Privacy Officer or Health Information Management (HIM) will amend the health record. The Veteran will be advised that their request has been approved and amendment changes will be recorded on the original document. Copies of the amended information will be provided to the Veteran and copies must be provided to all entities who have previously received a copy of the Veteran's health record, which can be determined through the accounting of disclosures.

When a request for amendment is denied, the VHA health care facility Privacy Officer will notify the Veteran in writing. This written response will state the reasons for the denial, including the appeal rights to the VA Office of General Counsel (OGC), and be signed by the VHA health care facility Director. The individual has the right to submit a statement of disagreement in response to the VHA health care facility's decision not to amend his/her health records prior to the completion of any appeals process. For additional information, contact the VHA health care facility Privacy Officer.

.

Right to an Accounting of 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 (Cite authority or applicable statute, etc.)

8. NAME AND TITLE OF VA EMPLOYEE MAKING THE DISCLOSURE

VA FORM JUN 2004 5572

AdobeFormsDesigner

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.

For additional information on maintaining an electronic spreadsheet, contact your VHA health care facility Privacy Officer.

Right to Confidential Communications

The Veteran has the right to request and receive communications confidentially from VHA by an alternative means or at an alternative location. VHA considers an alternative means to be an in-person request, and an alternative location to be an address other than the individual's permanent address listed in Veterans Health Information Systems and Technology Architecture (VistA).

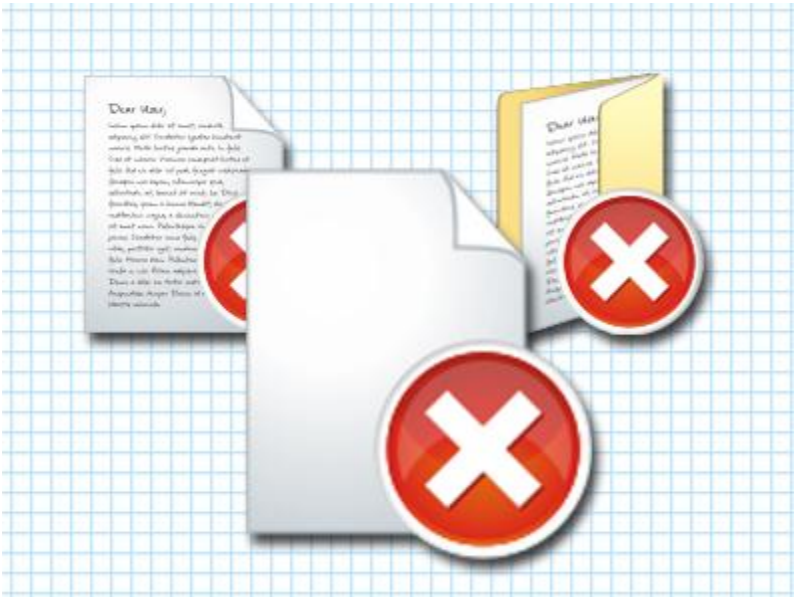
VHA shall accommodate reasonable requests from the individual to receive communications at an alternative address entered in VistA for one of the five correspondence types below:

- Eligibility or enrollment,
- Appointment or scheduling,
- Co-payments or Veteran billing,
- Medical records, and
- All other

Requests to send documents or correspondence to multiple addresses will be considered unreasonable and therefore denied (all or none to one address). All requests for confidential communication via e-mail will be denied.

Requests for confidential communications, in person or in writing, shall be referred to the appropriate office, such as eligibility or enrollment, for processing.

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. 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 op-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 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

Rights 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.

Right to File a Complaint

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

All privacy complaints should be referred to the VHA health care facility Privacy Officer for processing.

Module 2 Summary

Congratulations! You have completed Module 2.

In this module you learned about:

- The rights granted to Veterans,
- The rights of Personal Representative 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

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,
- Disclosing PHI for research purposes,
- Incidental Disclosures,
- Systems of Records and
- The process for releasing PHI from non-VHA Systems of 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.

Compensated work therapy (CWT) workers are not considered employees; therefore they cannot be giving access to Veteran PHI which is maintained by VHA. This includes computer systems and verbal or written access to PHI. These individuals cannot take privacy or security training so that they can have an employee status. These workers are **patients**. Appropriate placement for these workers would be grounds keepers, food service, and mail room mail sorter.

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

VHA may disclose PHI **including 38 USC 7332**-protected information to DoD for treatment purposes.

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

VHA may disclose Veteran PHI to:

- **Veterans Benefits Administration (VBA)** for eligibility for or entitlement to or to provide benefits under the laws administered by the Secretary of VA.
- **National Cemetery Administration (NCA)** for eligibility for or entitlement to or to provide benefits under the laws administered by the Secretary of VA.
- **Board of Veterans Appeals (BVA)** for eligibility or entitlement to or to provide benefits under the laws administered by the Secretary of Health.
- **VA contractors** as long as there is a business associate agreement in place.

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 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 (b4). Unions may request any records that are maintained by VHA facilities. This might include:

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

However, under certain circumstances, Unions may not be legally entitled to PHI or information protected by other statutes such as the Privacy Act. All requests for information by VA Union representatives are referred to the facility human resource management service.

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.

Employee Access to PHI Access

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"

Prepatory for 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 wavier of informed consent. In addition, the 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 your 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: 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 Principle investigator.

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 Veterans 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 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.

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 24VA19—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 Privacy Officer.

For a list of 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 Non-VHA System of Records

Within VHA facilities, there are several non-VHA systems of records that are subject to the provisions of the Privacy Act of 1974, VA Confidentiality Statutes and/or the HIPAA Privacy Rule.

For example, if a VHA employee produces a health record regarding a patient's claim for disability, this medical disability record is technically under the authority of the local VBA Regional Office. If your facility has disability claim health information such as Compensation and Pension exams refer to your health care facility Privacy Officer for disclosure guidance.

Note: Please see VHA Handbook 1605.1 *Privacy and Release of Information*, for a list of all non-VHA systems of records that are normally maintained within a VHA facility.

It is the policy of VHA that if a question arises concerning right of access, amendment or release of non-VHA records/information, the non-VHA System Manager (e.g., VBA, HRMS) who has responsibility over these records will be contacted. Whether or not right of access, amendment or release of the information is granted will be determined based on federal Privacy and Confidentiality Statutes, VA regulations, and official policies of the non-VHA entity.

VHA health care facility Privacy Officers should work with these offices to determine how to process such requests.

Module 3 Summary

Congratulations! You have completed Module 3.

In this module, you learned 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.

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

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.

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."

Authorization Requirements

If VHA employees receive a request for protected health information 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 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 must not be disclosed 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.

Processing 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 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 or a sensitive record review that has not been completed. For more information on the sensitive record review process or the VA police records exception, contact the VHA health care facility Privacy Officer.

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.

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

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: MCCF 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.

VBA CLAIMS FOLDERS: Requests for release of health information from the Veterans' VBA claims folders are normally handled by the FOIA/PA Officers at Veterans Benefits Administration (VBA) Regional Offices. A copy of the Compensation and Pension (C&P) exam located in VHA's health record can be disclosed directly to the Veteran.

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 session notes maintained by the psychotherapist 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: An individual does not have a "right of access" to these psychotherapy notes. For additional information contact your VHA health care facility Privacy officer.

Other Disclosures Requiring Authorization

TAKING VIDEO, PHOTOGRAPHS OR VOICE RECORDINGS:

In order for video, voice 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 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 VA Form 10-3203, *Consent for Use of Picture and/or Voice*. If the video, photograph or voice recording is going to be further disclosed than the patient must also sign VA Form 10-5345, *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 voice calls and the camera feature, to ensure and protect privacy of others, 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.

Module 4 Summary

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

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

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
- Federal Drug Administration (FDA)
- 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 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 the Chair of the Veterans' Affairs Committee or Subcommittee of the House of Representatives or the United States Senate without the individual's written authorization when the request for information is made part of the Committee health care oversight functions.

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 authorization. Disclosure of health information requires written authorization for a purpose other than described above.

Courts and Competency Hearings

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. Any subpoena for information received should be discussed with the VHA health care facility Privacy Officer and/or Regional Counsel.

If there is 38 USC 7332 information that is being requested then a very specific court order will be required. See your local VHA health care facility Privacy Officer and/or Regional Counsel for additional information.

Competency Hearings

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

Routine Reporting to Law Enforcement Entities Pursuant to Standing 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.

The health care facility Director or designee will acknowledge the receipt of an agency's standing written request letter and advise the agency of the penalties regarding the misuse of the information. The standing written request letter must be updated in writing every 3 years. See the VHA health care facility Privacy Officer for further information on standing written request letters.

Next of Kin, Family and Significant Others

VHA employees may disclose PHI to the next of kin, family, or significant other of an individual without prior written authorization General information on the individual's condition and location can be discussed if the individual has not opted out of the facility directory.

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 an 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 an 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.

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

Note: The minimum necessary standard does not apply to treatment purposes.

Non-VA Health Care Referral

VHA may disclose PHI **including** 38 U.S.C. 7332 protected information to a provider who has referred the Veteran for care as the referring provider already knows that the Veteran has the condition(s).

Organ Procurement Organization (OPO)

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.

This includes:

- 38 U.S.C. 7332 protected information
- Name and address of the patient to the local Organ Procurement Organization (OPO)
- Other entities designated by the OPO for inpatients whose death is imminent

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.

Food and Drug Administration (FDA)

VHA employees may disclose protected health information to the Food and Drug Administration (FDA) for the purpose of routine reporting and to carry out program oversight duties upon FDA's official written request.

State Veterans Homes

VHA employees may disclose protected health information, excluding 38 U.S.C. 7332 protected information, to a State Veterans Home for the purpose of medical treatment and/or follow-up at the State Home. VHA employees may disclose 38 U.S.C. 7332-protected information to a State Veterans Home only with the written authorization of the individual.

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 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://vaww4.va.gov/hia/UserGroups.htm.

Module 5 Summary

Congratulations! You have completed Module 5.

In this module you learned about:

- Disclosure procedures to non-VA entities.
- Disclosures to non-VA organizations

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
- Requirements for establishing new systems of records

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 Security Event Tracking System (PSETS) within one hour of discovery, promptly investigated and a written response provided to the complainant. In addition, all privacy complaints and incidents must be reported in PSETS. This is for audit purposes in accordance with VA Directive 6502, *VA Privacy Program*, and VHA Handbook 6502.1 *Privacy Violation Tracking System* (PVTS). Complaints are to be forwarded to the VHA health care facility Privacy Officer or the administration Privacy Office.

In addition, any Department of Health and Human Services Office for Civil Rights (HHS/OCR) complaints should be forwarded immediately to the VHA Privacy Office upon receipt of the complaint. Do not respond individually to an HHS/OCR complaint. The VHA Privacy Office will communicate with the VHA health care facility Privacy Officer and provide the response to the OCR investigator. It is crucial that the VHA health care facility Privacy Officer make every attempt to investigate and provide a response back to the VHA Privacy Office in a timely fashion.

Incidents

An incident is the act of violating an explicit or implied security policy including the notification of a suspected or actual loss, theft or inappropriate disclosure of personally identifiable information. An example of an incident is sending protected health information (PHI) via Outlook without encryption (e.g. Public Key Infrastructure (PKI) or Rights Management Services (RMS)) or finding protected health information (PHI) in unsecure boxes waiting to be shredded.

When employees discover an incident they are obligated to report these incidents to the VHA health care facility Privacy Officer, administration Privacy Officer, and/or the Information Security Officer (ISO) so that they can be reported in Privacy Security Event Tracking System (PSETS).

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*, for additional guidance.

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

VistA can be used to share PHI, 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 it includes PHI. Use secure messaging in MyHealtheVet for those communications that include PHI.

Note: The Veteran cannot give permission to communicate with them via email as it is against VA policy.

Contracts

Any contract between VHA and a contractor for the design, development, operation, or maintenance of a VHA system or any contract that necessitates the creation, maintenance, use, or disclosure of VA sensitive information will conform to the Federal Acquisition Regulations (FAR).

Organizations or individuals with whom VHA has a contract for services on behalf of VHA where VA sensitive information is provided to, or generated by, the contractors are considered business associates (See VHA Handbook 1600.01, *Business Associate Agreements*). Business associates must follow the privacy policies and practices of VHA.

All contractors and business associates and their employees must receive annual privacy training.

A review of the Statement of Work (SOW) and the signing of the checklist (Appendix C) from VA Handbook 6500.6, *Contract Security* must be done in order to be compliant. This review and sign off should be done collaboratively with the Information Security Officer (ISO), VHA health care facility Privacy Officer (PO) and the Contracting Officer.

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.

Health Information from Non-VA Physicians and Facilities

The Chief HIM or designee is responsible for the prompt dispatch of requests for health information available from outside sources and needed in the examination and treatment of VHA patients. Upon receipt, requested material must be made available to the health care practitioner without delay, when possible.

If the material is received in an electronic format, i.e., Compact Disk (CD), then the Chief HIM, or designee, should work with the facility Information Resource Management Service (IRMS) to check the CD for viruses and to ensure the facility has the appropriate software to open the files for review.

The health care practitioner must review the material to determine if inclusion in the individual's health record is warranted. If the health care practitioner determines the material should be included in the individual's health records, the Chief HIM, or designee, should determine the appropriate manner for inclusion in accordance with VHA Handbook 1907.01, *Health Information Management and Health Records*.

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.

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. When possible all required training should 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.

Module 6 Summary

Congratulations! You have completed Module 6.

In this module you learned about the requirements:

- For operational management and ensuring privacy when releasing information

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:

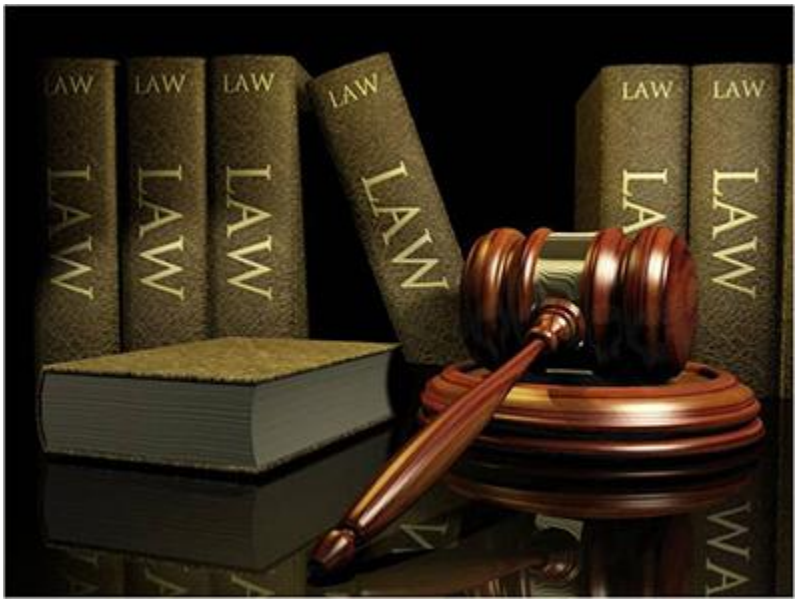
- Access
- Who Must Comply
- Who Can Make a FOIA Request
- Discretionary Disclosures and Government Transparency
- Procedural Steps
- Agency Records
- Time limits for a FOIA Request
- Consequences of Untimely Responses
- Expedited Processing
- Category of Requestors
- Fees and Fee Waivers
- Exemptions
- Appeals
- 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

- 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.

Amendments to the Act



- The Electronic Freedom of Information Act Amendments of 1996
  - All agencies are to make certain types of records, created by the agency on or after 11/1/1996, available electronically.
  - Required agencies to establish electronic reading rooms for citizens to use to have access to records.
  - Extended the agencies required response time to FOIA requests from 10 work days to 20 work days.
- Executive Order (E.O.13,392) – 12/14/2010 – Improving Agency Disclosure of Information
  - Calls upon all agencies to improve their FOIA operations with both efficiency and customer service in mind.
- Open Government Act – 12/31/2010
  - Promote accessibility, accountability and openness in Government.
  - Created the Office of Government Information Services (OGIS), within the National Archives and Records Administration (NARA).
    - Review policies and procedures of agencies FOIA.
    - Review compliance with the statute and recommend policy changes to Congress and the President to improve the administration of FOIA.
    - Offer mediation services to resolve disputes between persons making FOIA requests and agencies.
    - FOIA Ombudsman – Intermediary between the agency and the requester.

Access

The FOIA requires disclosure of VA records, or any reasonable portion of a record that may be segregated, to any person upon written request. VHA administrative records will be made available to the greatest extent possible in keeping with the spirit and intent of the FOIA.

Before disclosing records in response to a FOIA request, the record will be reviewed to determine if all or only parts of it can be disclosed.

Records or information customarily furnished to the public in the regular course of the performance of official duties may be furnished without a written request. A request for access to official records under the FOIA must be in writing and reasonably describe the records so that they may be located.

Who Must Comply?

- All agencies within the executive branch of the federal government, including the Executive Office of the President and independent regulatory agencies.
- Not required:
    - State governments
    - Local governments and municipalities
    - Foreign governments
    - Courts
    - Congress
    - Presidential Transition Teams
    - Offices within the Executive Office of the President whose functions are limited to advising and assisting the President.
        - Including Office of the President and Vice President

Note: this is an AGENCY responsibility, not just the responsibility of the FOIA Officer.

- Employee responsibilities in searching for agency records subject to FOIA requests should be clearly addressed in your local FOIA policy.
- FOIA Officers should meticulously document the search efforts of all staff searching for responsive records. All search documentation should be maintained in the FOIA administrative record.

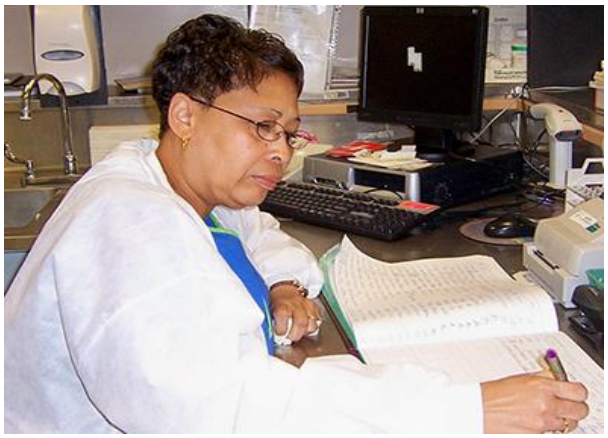
Who Can Make a FOIA Request?

- Virtually ANYONE!
- Exceptions:
    - Federal agencies may not use the FOIA as a means of obtaining information from other federal agencies
    - Congress 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
    - Foreign governments when made to intelligence organizations. (Intelligence Authorization Act of 2003)
- Includes:
    - Private citizens
    - Members of Congress
    - Corporations, associations, partnerships
    - Foreign and domestic governments
    - Unions
    - Other federal employees

Discretionary Disclosures and Government Transparency

- When processing FOIA requests, there is a "clear presumption of disclosure."
- Information should not be kept confidential merely because:
    - Officials might be embarrassed;
    - Errors or failures might be revealed, or
    - Because of speculative or abstract fears.
- Agencies are strongly encouraged to make discretionary disclosures of information.
- All exemptions are discretionary; however, if a federal statute mandates or requires the withholding of information, the application of the exemption is not discretionary. For example, if a requestor seeks the names and home addresses of all Veterans, the disclosure is prohibited by 38 U.S.C. 5701 and thus the application of Exemption 3 is not discretionary.
- Currently, the Department of Justice will only defend agencies withholding information when:
    - The agency reasonably foresees that disclosure would harm an interest protected by one of the statutory exemptions, or
    - Disclosure is prohibited by law.

Procedural Steps



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/.

- The facility or administration FOIA Officer will review the request to determine compliance with the FOIA and the VA's implementing regulations. The facility or administration FOIA Officer will take the following actions:
    1. The request should be date stamped.
    2. Create administrative file
    3. Once the request is received by the appropriate FOIA Office, the FOIA request should be logged into FOIAXpress.
    4. Make a determination if the request is being sent to the correct agency component.
    5. Determine if clarification is needed on any aspect of the request.
        - If clarification is needed, you should always document your understanding of the clarification in writing to the requestor.
    6. Section 7 of the Open Government Act requires that agencies provide acknowledgment of a FOIA request within 10 work days.
    7. Acknowledge the request.
    8. Issue decisions on expedited processing and fee waivers, if requested.
    9. Issue fee estimate, if applicable.
    10. Issue records search assignment.
- 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.
- Upon receipt of the records, the facility or administration FOIA Officer will take the following actions:
    1. Photocopy records and maintain an original, unredacted copy for the FOIA administrative file.
    2. Review and redact records in accordance with FOIA exemptions and make a copy of the redacted records for the FOIA administrative file.
    3. Issue initial agency decision, providing appeal rights if necessary.
    4. Process and close request in FOIAXpress.
    5. Organize and compile a FOIA administrative file for maintenance in accordance with VHA's records retention schedule.

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.

What Agency Records Are Not...

- Objects (furniture, wall paintings, etc.)
- Non-Tangibles (an individual's memory or oral communications)
- Personal records of an individual that are:
    - Maintained for the convenience of the employee **and**
    - Not subject to record retention and disposal rules.
    - Private material brought into the agency for employee's reference.
- Notes created by supervisors and other employees provided they are:
    - Not filed with official records **and**
    - Not shared with other employees **and**
    - Not required by law, regulation or custom to be created **and**
    - Not used in the decision-making process.

Time Limits for a FOIA Request

A request for records received will be promptly referred for action to the appropriate VA FOIA Office. 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 search 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.

Expedited Processing

- A FOIA requestor may ask in writing for "expedited processing" of a FOIA request for a demonstrated "compelling need."
- There are two compelling needs:
    - Failure to obtain records quickly "could reasonably be expected to pose an imminent threat to the life or physical safety of an individual," or
    - The requestor demonstrates "an urgency to inform the public concerning actual or alleged Federal Government activity."
- The FOIA Office must decide whether to grant a request for expedited processing within 10 calendar days of receiving the request.
- If the FOIA Office denies the request, the office must immediately notify the requestor of that decision in writing, including the right of the requestor to appeal the decision denying the request for expedited processing.
    - When the Agency grants a request for expedited processing, the FOIA Officer must move the expedited request to the top of their processing queue.

Categories of Requestors, Fees, and Fee Waivers

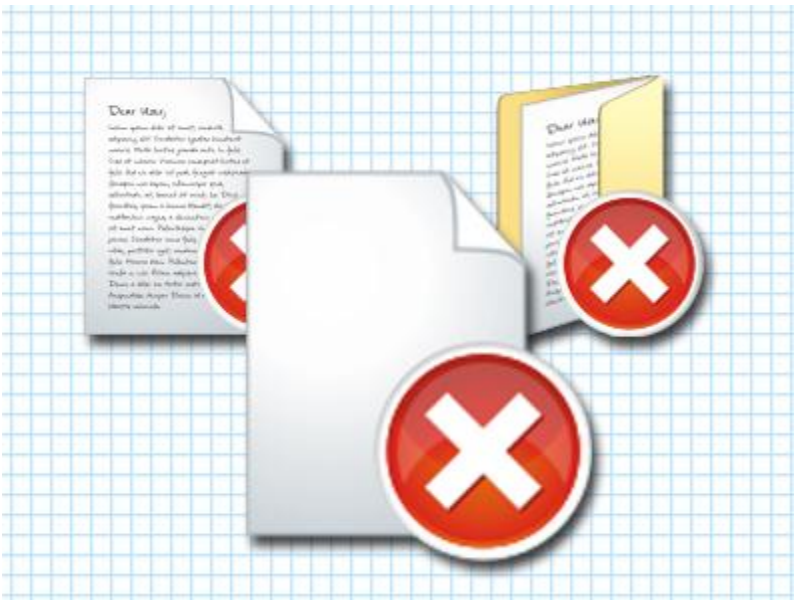
- **There are three categories of requestors for fee-related purposes**:
  - *Commercial Use Requestors*: Commercial use requestors are charged for all search, review and copying costs.
  - *Educational Institutions, Noncommercial Scientific Institutions and Representatives of the News Media*: Educational institutions, noncommercial scientific institutions and representatives of the news media are only charged copying costs after receiving the first 100 one-sided pages free.
  - *All Other Requestors*: All other requestors are charged search and copying costs after receiving the first two hours of search time free and the first 100 one-sided pages free.
- **The FOIA provides for three categories of fees that may be charged in response to FOIA requests:**
  - *Document Search Costs*, including all the time spent looking for responsive material.
  - *Review Costs*, which consists of the direct costs incurred during the initial examination of a document for the purposes of determining whether it must be disclosed under the FOIA.
  - *Duplication or Copying Costs*, which represent the reasonable "direct costs" of making copies of documents.

    Limitation on Fees

  - Section 6 of the Open Government Act prohibits agencies from assessing search fees (or duplication fees if the requestor is an educational or noncommercial scientific institution or a representative of the news media) if the agency fails to meet the 20 work day response time limit, unless:
    - Unusual circumstances
    - Exceptional circumstances

- **Fees and Fee Waivers**
  - FOIA fees can be waived or reduced in response to a request for a fee waiver or reduction when it is determined that furnishing the requested record(s) is:
    - In the public interest because disclosure is likely to contribute significantly to the public understanding of the operations and activities of the government; and,
    - Is not primarily in the commercial interest of the requestor.
  - Because the requestor must be in a position to disseminate the information requested to members of the general public, those eligible for fee waivers and reductions are primarily limited to representatives of the news media.
    - Some requestors may be considered even though they are not news organizations based upon their ability to disseminate information to news sources (i.e. government watch groups).

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

Appeals

VA's Office of the General Counsel (OGC) serves as the appeal authority for receiving and processing appeals submitted by a requestor.

When the VA OGC receives an appeal, the facility FOIA Officer who processed the initial FOIA request will be notified.

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 comply with the guidance and direction provided by 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).

Module 7 Summary

Congratulations! You have completed Module 7.

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

- Access
- Who Must Comply
- Who Can Make A FOIA Request
- Discretionary Disclosures and Government Transparency
- Procedural Steps
- Agency Records
- Time limits for a FOIA Request
- Consequences of Untimely Responses
- Expedited Processing
- Category of Requestors
- Fees and Fee Waivers
- Exemptions
- Appeals
- Litigation
- The Annual Report of Compliance

Course Summary

During this course, you have learned about:

1. Basic Privacy Laws and Regulations
2. Veterans Rights
3. Uses and Disclosures of Information in VA
4. Purposes that Require an Authorization
5. Releases of Information Outside of VA
6. Operational Privacy Requirements and
7. Freedom of Information Act (FOIA)

- **Congratulations! You have completed all seven modules. Please follow the instructions listed below:**
- **Please print your Certificate of Completion**
- **Sign it and have your**
- **Supervisor sign it and**
- **Keep copy for your records.**

Certificate of Completion
Privacy and HIPAA Training

I, _____ certify that I completed the Privacy and HIPAA training on

Date _____.

Signature of employee/Contractor

Signature of Supervisor / Date