

# Privacy and HIPAA Focused Training – FY2016

## Welcome and Introduction

Welcome to the Privacy and HIPAA Focused Training Web Site. This course is designed to be finished in 50-60 minutes.

### Note:

**If you experience technical problems or need assistance while you are going through the training contact the VA Talent Management System (TMS) Help Desk at [vatmshelp@va.gov](mailto:vatmshelp@va.gov) or Monday through Friday between 08:00A - 10:00P at 1-866-496-0463.**

### Audience

All staff with direct access to protected health information (PHI) or access to PHI through VHA computer systems is required to complete this training annually.

All new employees with direct access to PHI or access to PHI through VHA computer systems are required to take this training within 30 days of hire or prior to the employee being allowed access to PHI in any format.

A team of subject matter experts from the VHA Privacy Office have created this training.

### Goals

The goal of this training is to provide knowledge of:

- Module 1 – Basic Privacy Statutes and Employee Responsibilities
- Module 2 – Veteran's Rights
- Module 3 – Introduction to Uses and Disclosures of Information
- Module 4 – Authorization Requirements and Privacy of photographs, digital images and video and audio recordings
- Module 5 – Special Privacy Topics
- Module 6 – Freedom of Information Act (FOIA)

### Course Structure

This course is divided into modules. Modules are divided into smaller sections called topics. Additional Privacy policy-related content is provided using the following methods:

When going through the training, select the [NEXT] button once and wait for the page to load. Selecting the [NEXT] button multiple times may cause the pages to load incorrectly.

Your knowledge of the training content will be checked periodically. You must answer each Knowledge Check question correctly in order to proceed with the training.

### NOTE:

**It is imperative to read instructions and the question text thoroughly.**

**The complete Privacy and HIPAA Focused Training is accessible from all screens by selecting the resource link available on the navigation bar of each page.**

## Bookmarking

You may exit the training at any time by clicking the **[EXIT]** button at the top-right of the screen.

If you leave this training before you have completed all the lessons, your progress is saved. When you log back in and go to the Online Content Course screen, click the yellow **[LAUNCH AGAIN]** button to return to the training.

Then, a message box will appear asking "Do you want to go back to the last page you were on earlier?" Click the **[OK]** button to resume where you left off.

Alternatively, you may select the **[MENU]** button and jump to the beginning of each module. Notice that your progress is recorded by a checkmark next to each module title.

## Navigation

The training is navigated using the **[NEXT]** or **[BACK]** buttons.

Please take the training in sequential order.

The following buttons are accessible throughout the training:

Name of Button	Keyboard Shortcut	Description
<b>BACK</b>	ALT+4	Return to the previous content screen
<b>NEXT</b>	ALT+5	Proceed to the next content screen
<b>EXIT</b>	ALT+0	Log out of the training
<b>GLOSSARY</b>	ALT+3	Open an alphabetical list of glossary terms
<b>HELP</b>	ALT+2	Open help content

# Lesson 1: Basic Privacy Statutes and Employee Responsibilities

## Lesson Objectives

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:

Seven statutes that govern the collection, maintenance and release of information from Veterans Health Administration (VHA) records,

Employee responsibility in the use and disclosure of information,

Unauthorized Use, Access or Disclosure of Personally Identifiable or Protected Health Information, and

Functional Categories and Minimum Necessary Standard

## Basic Privacy Statutes

VHA health care facilities should comply with all statutes simultaneously 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.

Basic Privacy Statutes	Description
<b>The Privacy Act (PA), 5 U.S.C. 552a</b>	The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.
<b>Health Insurance Portability and Accountability Act (HIPAA)</b>	The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.
<b>Health Information Technology for Economic and Clinical Health (HITECH) Act</b>	The Health Information Technology for Economic and Clinical Health (HITECH) Act addresses the privacy and security concerns associated with the electronic transmission of health information.
<b>38 U.S.C. § 5701 VA Claims Confidentiality Statute</b>	38 U.S.C. Section 5701 makes VA benefits records and the names and home addresses of present and former armed forces personnel and their dependents confidential.
<b>38 U.S.C. § 5705 Confidentiality of Healthcare Quality Assurance Review Records</b>	38 U.S.C. 5705 Confidentiality of Healthcare Quality Assurance Review Records makes information and records generated by VA's medical quality assurance program confidential and privileged and exempt from disclosure under the FOIA.

<b>38 U.S.C. § 7332 Confidentiality of Certain Medical Records</b>	38 U.S.C. Section 7332 makes strictly confidential all VA records that contain the identity, diagnosis, prognosis or treatment of VA patients or subjects for drug abuse, alcoholism or alcohol abuse, infection with human immunodeficiency virus (HIV/AIDS), or Sickle Cell Anemia.
<b>The Freedom of Information Act (FOIA), 5. U.S.C. 552</b>	The FOIA requires Federal departments and agencies, such as VA, to release their records unless FOIA specifically exempts the information or record from disclosure.

## Employee Responsibility in the Use and Disclosure of Information

- VHA employees must comply with all Federal laws and regulations, VA regulations and policies, and VHA policies regarding the confidentiality and privacy of Veteran and employee records. In addition, all VHA employees must conduct themselves in accordance with the rules of ethical conduct.
- Personally identifiable information (PII) and protected health information (PHI) on Veterans and employees should only be collected, accessed or viewed by VHA employees with a need for that information in the performance of their official VA duties for payment, treatment or health care operations. VHA employees should not access or view the PII/PHI of their coworkers or Veterans out of curiosity or for any purpose that is not related to official VA duties for payment, treatment or health care operations. Also, Supervisors may not view the health records of their employees who are Veterans to look at their clinic appointments or other health information for employment-related purposes.
- VHA employees who collect, access, or view PII/PHI on Veterans or employees for purposes other than those for official VA duties, including curiosity, are subject to disciplinary action. Even if the VHA employee had good intentions in accessing or viewing the Veteran or employee information, such as to look up a home address to send a sympathy card, it is a privacy breach and disciplinary action may result.

## Unauthorized Use, Access or Disclosure of Personally Identifiable or Protected Health Information

The following are examples of unauthorized use that will result in appropriate disciplinary action:

- Accessing information outside the scope of your functional category.
- Checking a co-worker's health record upon their request without a business need to know.
- Checking family members' health records without a business need to know.
- Checking Veteran's or employee's health records out of curiosity.
- Supervisors can no longer access their employee Veterans' health records under a need to know.

The following are potential administrative actions that may be taken by the supervisor with guidance from Human Resources:

- Reprimand being placed in personnel file,
- Suspension from job,
- Demotion, or job loss,
- Civil or criminal prosecution, or

- Fines or imprisonment

## Functional Categories and Minimum Necessary Standard

*VHA Handbook 1605.02* "Minimum Necessary Standard for Protected Health Information" discusses the requirement for assignment of functional categories. The handbook states that VHA must identify the persons, or classes of persons, who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.

VHA personnel must be assigned a functional category by their supervisor upon initial hire, position change, and annually thereafter to review the applicability of access to protected health information to their official job duties.

VA form 10-0539, "Assignment of Functional Categories" is found in *VHA Handbook 1605.02 Appendix E* and can be used to assign functional categories. **Employees must sign and date the form annually.**

The form is not required to be used but if it is not used a documented process must be in place to ensure compliance. Refer to your local facility Privacy Officer for additional guidance.

## Lesson 2: Veterans Rights

### Lesson Objectives

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 Veterans 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 Disclosures,
- Request and receive confidential communications,
- Request restriction of use or disclosure of records, and
- File a complaint

### **IMPORTANT:**

**These rights extend to the personal representative of a deceased individual (e.g. Executor of the Estate, Next of Kin).**

**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.**

### 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.

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 Privacy Officer or at the following website:

[http://www1.va.gov/vhapublications/ViewPublication.asp?pub\\_ID=3048](http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=3048).

### Right of Access

A Veteran has a right to obtain a copy of his or her own health record. A Veteran must submit a **signed written request** to the VHA health care facility where the record is maintained.

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, without a written request, if it is for patient education purposes or discharge planning. If the Veteran is requesting their health information for previous progress notes or labs, they must submit a written request and be referred to the facility release of information office. Veterans

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.

## 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. Requests for amendments to health records should be directed to the local Privacy Officer or Chief of Health Information Management Service (HIMS). Authors of the requested amendments should work with their Privacy Officers or Chief of HIMS so that a timely response is given.

## 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 program offices are required to keep an accurate accounting for each disclosure made to a party external to VHA. An accounting is not required to be maintained in certain circumstances, including when the disclosure is to VHA employees who have a need for the information in the performance of their official duties, if the release is to the individual to whom the record pertains or the release of information is pursuant to a FOIA request.

Entry of a VA patient by name or other identifier into a State Prescription Drug Monitoring program is considered a disclosure that must be accounted for. The employee making the disclosure must do the accounting of disclosures; this can be done through creating a note in CPRS or accounting for the disclosure manually. Work with your VHA facility Chief of HIMS for additional guidance.

Electronic batch reporting by the IT system will capture the information that can be used to generate the accounting of disclosures retrospectively when requested. Check with your local OI&T for the status of electronic batch reporting.

## 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 any of the five correspondence types below:

- Eligibility or enrollment,
- Appointment or scheduling,
- Co-payments or Veteran billing,
- Health 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).

Requests for confidential communications, in person or in writing, shall be referred to the appropriate office, such as eligibility or enrollment, for processing. All requests for confidential communication via e-mail will be denied.

### **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. Documenting in the CPRS health record does not constitute a valid restriction request.

VHA **is not required** to agree to such restrictions, but if it does, VHA must adhere to the restrictions to which it has agreed. A request for restriction should be delivered to the Privacy Officer or designee for processing.

### **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, staff is required to ask the individual their preference about opting out of the facility directory.

### **Right to File a Complaint**

Patients have a right to file a complaint if they believe that VHA has violated their (or someone else's) health information, privacy rights or committed another violation of the Privacy or Security Rule.

A complaint can be filed by contacting one or more of the following:

- The VHA health care facility's Privacy Officer, where they are receiving care,
- The VHA Privacy Office,
- Office of Inspector General, or
- The U.S. Department of Health and Human Services, Office for Civil Rights



## Lesson 3: Introduction to Uses and Disclosures of Information

### Lesson Objectives

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 or disclosing PHI for treatment, payment and/or health care operations (TPO),
- Disclosure of PHI without an authorization for other than TPO,
- Use of PHI for research purposes,
- Incidental Disclosures, and
- 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**.

"Treatment" generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

"Payment" encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

"Health care operations" are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.

### Disclosure of PHI without an Authorization for Other than Treatment, Payment, or Health Care Operations

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)
- National Cemetery Administration (NCA)
- Board of Veterans Appeals (BVA)
- VA contractors (as long as there is a business associate agreement in place)

### Disclosure of PHI without an Authorization for Other than Treatment, Payment, or Health Care Operations, continued

There are also a number of situations where VHA may disclose information, without an authorization, for other than treatment, payment, or health care operations. Examples of some of these include:

- Public Health Activities (e.g., giving information about certain diseases to government agencies)

- When Required by Law
- Research Activities (e.g., giving information to a researcher to prepare a research protocol)
- Abuse Reporting (e.g., giving information about suspected abuse of elders or children to government agencies)
- Law Enforcement
- State Prescription Drug Monitoring Program (SPDMP)

For additional information and guidance contact your Privacy Officer.

## Use of PHI for Research Purposes

A VA researcher may access PHI without the subject's written authorization if the information is reviewed preparatory to research on human subjects. 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 Institutional Review Board (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 reviewed by the 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, the Informed Consent (10-0086) must state that a photograph, image or video/audio recording is going to be made. If the documentation of ICF is waived, the script for the audio-recording must include the subject's permission to be recorded.

## Incidental Disclosures

Many customary health care communications and practices play an 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.

### NOTE:

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

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;
- Using Veteran's ID card for identification of the patient, instead of asking for their SSN, when it is available;

- Using Kiosks, where available, when checking in for an appointment instead of lining up at the check in desk.

## System of Records

A System of Records (SOR) is a group of records under the control of the agency from which information about an individual is 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 information 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>.

# Lesson 4: Authorization Requirements and Privacy of photographs, digital images and video and audio recordings

## Lesson Objectives

In this module, you will learn the components for a valid authorization and information about the privacy of audio and video recordings.

Specifically, you will learn about:

- Authorization Requirements, and
- Privacy of photographs, digital images and video and audio recordings

## Definition of Authorization

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 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.

## Authorization Requirements

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.

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 a need or an event,
- Include a statement that the patient may revoke the authorization in writing, except to the extent the facility has already acted in reliance on it, and a description of how the individual may revoke the authorization,
- Include a statement that treatment, payment, enrollment, or eligibility for benefits cannot be conditioned on the individual completing an authorization, and
- Include a statement that the information may no longer be protected from re-disclosure.

If any of the authorization requirements listed above have not been satisfied the authorization will be considered invalid.

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.

### NOTE:

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

## Privacy of Photographs, Digital Images and Video and Audio Recordings

The facility must post obvious signage at each entrance of the facility clearly stating the local policy regarding photography, digital imagery, or video/audio recording guidelines.

**VA Form 10-3203, Consent for Production and use of Verbal or Written Statements, Photographs, Digital Images, and /or Audio Recordings by VA must be obtained when a personally identifiable image, likeness, or recording of a member of the VHA workforce is produced or used by VHA for official purposes.**

- VA Form 10-3203 is not needed when staff communications using teleconferencing, video-conferencing, or other similar platforms are taken for official purposes. The consent is not needed whether or not the equipment and software are capable of producing photographs, digital images, or recordings that are accessible at a later time.
- Participants of office functions, staff meetings or holiday parties should be told they may be subject to photography, imaging, or recording. A consent form is not required.
- No personally identifiable image, likeness, or recording of members of the VHA workforce is included in a photograph, digital image, or video or audio recording produced and used by VHA unless the person gives written consent.

**VA Form 10-3203a, Informed Consent and Authorization for Third Parties to Produce or Record Statements, Photographs, Digital Images, or Video or Audio Recordings when an individual is going to be interviewed by a third party.**

Consent is required for Official Purposes such as the following but are not limited to performance improvement, quality improvement, health care operations, payment activities, legal services, and determinations of eligibility for VA benefits (including compensation and pension examinations).

More examples of activities undertaken for official purposes include but are not limited to certain education activities (e.g., development of educational brochures, face-to-face or virtual training videos and materials, biographies on web sites; communication; outreach, including promoting services using a patient or group photograph in facility newsletters, facility outreach programs, or social media; or preparation of publications.

### **NOTE:**

**VHA employees may not secretly take pictures or record conversations without proper consent of the other party. See VHA Directive 1078 "Privacy of Persons Regarding Photographs, Digital Images, and Video or Audio Recordings" for additional guidance.**

## Lesson 5: Special Privacy Topics

### Lesson Objectives

In this module, you will learn about several special privacy topics that have not been discussed in previous modules.

Specifically you will learn about:

- Release of 38 U.S.C. § 7332 Information
- Compensated Work Therapy (CWT)
- Subpoenas
- Logbooks
- Whistleblower
- Compliance
- Virtual Lifetime Electronic Record (VLER)

### Release of U.S.C. §7332 Protected Health Information, part 1 of 2

38 U.S.C. Section 7332 makes strictly confidential all VA records that contain the identity, diagnosis, prognosis or treatment of VA patients or subjects for drug abuse, alcoholism or alcohol abuse, infection with human immunodeficiency virus (HIV/AIDS), or Sickle Cell Anemia. This statute applies to information whether or not it is recorded in a document or a Department record.

For example, a VHA health care provider's conversation discussing a patient's diagnosis, prognosis, and treatment would be protected by Section 7332. Finally, this statute protects records and information of the testing of individuals for HIV infection and sickle cell anemia, including negative test results.

Before making a disclosure of any 38 U.S.C. §7332 protected health information to an outside entity without an individual's authorization, VHA employees should determine:

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

### Release of U.S.C. §7332 Protected Health Information, part 2 of 2

The following is a list of examples when 38 U.S.C. § 7332 information **cannot** be disclosed without specific authorization such as a signed authorization from patient, standing written request letter, or written request.

- To non-VA health care providers (e.g. physicians, hospitals, clinics, and nursing homes) for treatment purposes or payment services.
- To an insurance company for payment purposes.
- 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.
- In court orders if there is 38 U.S.C. § 7332 information being requested a very specific court order will be required. Please consult your Regional Counsel.
- 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.
- For the purpose of health care referrals, to resident care homes, assisted living facilities, and home health services.

- To Federal, State, and/or local public health authorities, for HIV reporting only, charged with the protection of the public health or safety pursuant to a standing written request letter or other applicable legal authority. Please consult your Privacy Officer.

The following is a list of situations where 38 U.S.C. § 7332 allows for the release of information without a signed authorization:

- For health care oversight activities a written request is not required and VHA may only disclose 38 U.S.C. § 7332 protected health information to the OIG for health care oversight activities.
- 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.

## Compensated Work Therapy (CWT)

Compensated work therapy (CWT) program members 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 individuals enrolled in the CWT program should 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.

## Subpoenas

A subpoena is a document issued by or under the auspices of a court seeking a release of records or requesting an individual give testimony before a court of law. A subpoena must be signed by a judge for VHA to disclose Privacy Act-protected records.

The facility Privacy Officer and Regional Counsel must be notified in all cases where any personnel receive a court order for the production of records or a subpoena for records.

## Logbooks

A physical logbook is any written (i.e., not electronic) record of activities or events comprised of data which may uniquely identify an individual or contain sensitive personal information that is maintained over a period of time for the purpose of monitoring an activity, tracking information or creating a historical record. The following are examples of physical logbooks:

- Respiratory therapy logs
- Laboratory logs
- Autopsy logs
- Wound care logs
- Logs of cases cleared
- Printouts of Excel spreadsheets
- Access data base printouts

Physical logbooks containing sensitive personal information can only be created, used and maintained for a compelling business need as approved by the VHA facility director or the Program Office Director. A compelling business need is one that requires the capture of sensitive personal information for a policy, regulatory, accreditation or statutory requirement. Compelling business needs may support reasonable and appropriate business operations, patient safety or quality improvement efforts, or other prudent and important health care

operations needs such as the board certification of clinical staff including residents and trainees. Transition of physical logbooks to secure electronic logbooks and tracking systems is highly encouraged.

Physical logbooks are vulnerable to loss, theft or misuse of logbook content. Loss of control over a logbook can result in the compromise of sensitive personal information for multiple individuals, which could put individuals at risk for financial, reputational, or other harm and may result in a loss of trust in VHA's ability to secure sensitive personal information.

## Whistleblower

In order to have legal authority for disclosure of protected health information and not violate any federal privacy law or regulation, a Whistleblower, which is a member of the VA workforce or VHA business associate who, in good faith, believes that VHA has engaged in conduct that is unlawful or otherwise violates professional or clinical standards; or that the care, services, or conditions provided by VHA potentially endangers one or more patients, workers, or the public, may disclose protected health information to:

- A health oversight agency, such as VA OIG, Congressional Committees (e.g., House Veterans Affairs Committee and Senate Veterans Affairs Committee) and the Office of Special Counsel, authorized by law to investigate or otherwise oversee the relevant conduct or conditions of VHA;
- A public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of VHA;
- An appropriate health care accreditation organization, such as The Joint Commission, for the purpose of reporting the allegation of failure to meet professional standards or misconduct by VHA; or
- An attorney retained by or on behalf of the VA workforce member or VHA business associate for the purpose of determining the legal options of the VA workforce member or VHA business associate with regard to the conduct described above.

### NOTE:

**An employee who discloses protected health information to an entity other than those listed above and will be considered to have made an unauthorized disclosure in violation of the Privacy Act, HIPAA Privacy Rule and VHA policy. Such unauthorized disclosure can result in disciplinary action. For additional guidance contact your facility or administrative Privacy Officer.**

## 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 D.

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 1605.02, "Minimum Necessary Standards for Protected Health Information" for additional guidance.

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.



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.

## **Virtual Lifetime Electronic Record (VLER)**

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 eHealth Exchange to share prescribed patient information via this protected network environment with participating private health care providers, but this does not involve 'scanned' patient information.

VLER benefits Veterans who receive a portion of their care from non-VA health care providers. Below are some of the benefits:

- Eliminates need to hand-carry health records.
- Allows VA and private health care providers to share access of up-to-the-minute health information.
- Veterans may opt-in or opt-out at any time.
- 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).

# Lesson 6: Freedom of Information Act (FOIA)

## Lesson Objectives

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
- Agency Records
- Employee Responsibilities
- Who Can Make A FOIA Request

## Elements of FOIA

The basic purpose of the Freedom of Information Act (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.

## Agency Records

A valid FOIA request must be in writing and may be received by mail, e-mail, by hand or fax. Requests made under the FOIA must reasonably describe the records being requested. If VHA employees receive FOIA requests for any type of agency records they should be forwarded to the VHA healthcare facility's FOIA Officer.

## 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.

## Employee Responsibilities

The FOIA Officer will make all determinations regarding release of the requested records and employees must fully cooperate with the FOIA Officer in the handling of these requests.

- Specific employee responsibilities include:
  - Searching for agency records at the direction of the 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

- Being accessible to the FOIA Officer for questions/clarifications
- Compiling 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.

You may find the appropriate FOIA Officer using the FOIA Officer Contact roster on the VA FOIA Homepage at <http://www.foia.va.gov/>.

## Who Can Make a FOIA Request?

Virtually ANYONE, including:

- Private citizens
- Members of the media
- 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

The only exceptions to the above items are:

- 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

## Exemptions

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.

## Course Summary

During this course, you have learned about:

- Basic Privacy Statutes and Employee Responsibilities
- Veterans Rights
- Introduction to Uses and Disclosures of Information
- Authorization Requirements and Privacy of photographs, digital images and video and audio recordings
- Special Privacy Topics
- Freedom of Information Act (FOIA)

## Course Conclusion

This concludes the Privacy and HIPAA Focused Training for FY2016.

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

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

Thank you for your participation.