Name of Volunteer _____ Date_____

Department Of Veterans Affairs Voluntary Services Orientation Checklist

❑ Steps to fill out Application for Voluntary Service

- Fill out **Application for Voluntary Service**.
- Fill out **Orientation Answer Sheet**. To access the training manual, Log on to the following web site:

  http://www.boise.va.gov/giving/index.asp

  - Scroll down to where it says VA Voluntary Service Orientation Booklet. Questions are in the back of each training module. Fill out the answer sheet in the packet. Mark the answer that most accurately answers the questions.
- Read **Privacy and HIPAA Focused Training,** and **VA Privacy & Information Security Awareness & Rules of Behavior for Volunteers**, *sign the Certificate of Completion*.
- Read and sign **Voluntary Service Dress Code**
- **Declaration for Federal Employment.** Volunteers are considered employees without compensation. Please ***fill out the*** form, in preparation to be fingerprinted if you are 18 or older.
- Read & sign **Personal Identification Verification Card (PIV) Training Document**.
- Fill out highlighted areas on the **Request for Personal Identity Verification Card.**

***Before proceeding*, email Voluntary Service**
BOIVoluntaryService@va.gov
to schedule an appointment to go over your completed packet. If you do not have email please call 422-1176.

Employee Health TB Test

Date Given: _____

Date Read: _____

Please date, initial and return to volunteer.

Human Resources received paperwork:

Date: _____

Received by: _____

Please date, sign and return to volunteer.

❑ Steps to complete Volunteering Process

❑ Blood Draw for Tuberculosis

- We will get your test done when your fingerprints clear and you come back in for the picture for your badge.
- You must be tested no later than 2 weeks after you start volunteering.

❑ Background check (required) for 18 and over.

- An appointment will be made for you to have your fingerprints taken. You will return your packet 30 minutes prior to fingerprinting to Voluntary Service. You will go to Human Resources, (Bldg. 24).
- Bring the Declaration for Federal Employment and a copy of your volunteer application (form 10-7055), and this checklist.
- Fingerprinting takes on average about 10 to 15 business days to be processed.

❑ Volunteer Badge

- After your fingerprints come back we will contact you in regards to getting your ID badge. You will need to set an appointment up for your photo ID (Bldg. 24) (208) 422-1000, ext. 7211. Bring two forms of legal ID to the appointment.

❑ Volunteer Hours

- You will receive 12 hours of volunteer work for completion of this process.
- Voluntary Service will give you a code so you can enter your hours in the computer in the Escort/Messenger room on the days you are volunteering.
- If working after hours or on the weekend please keep track of your hours and at the end of the month turn them in to the Voluntary Service Office.

❑ **Flu Shot (Required)** to volunteer.

❑ Procedure for Leaving Voluntary Service

- Notify your supervisor when you decide you will no longer be volunteering.
- Return your ID badge and vest/jacket to Voluntary Service, Building 85A, Room 1102.

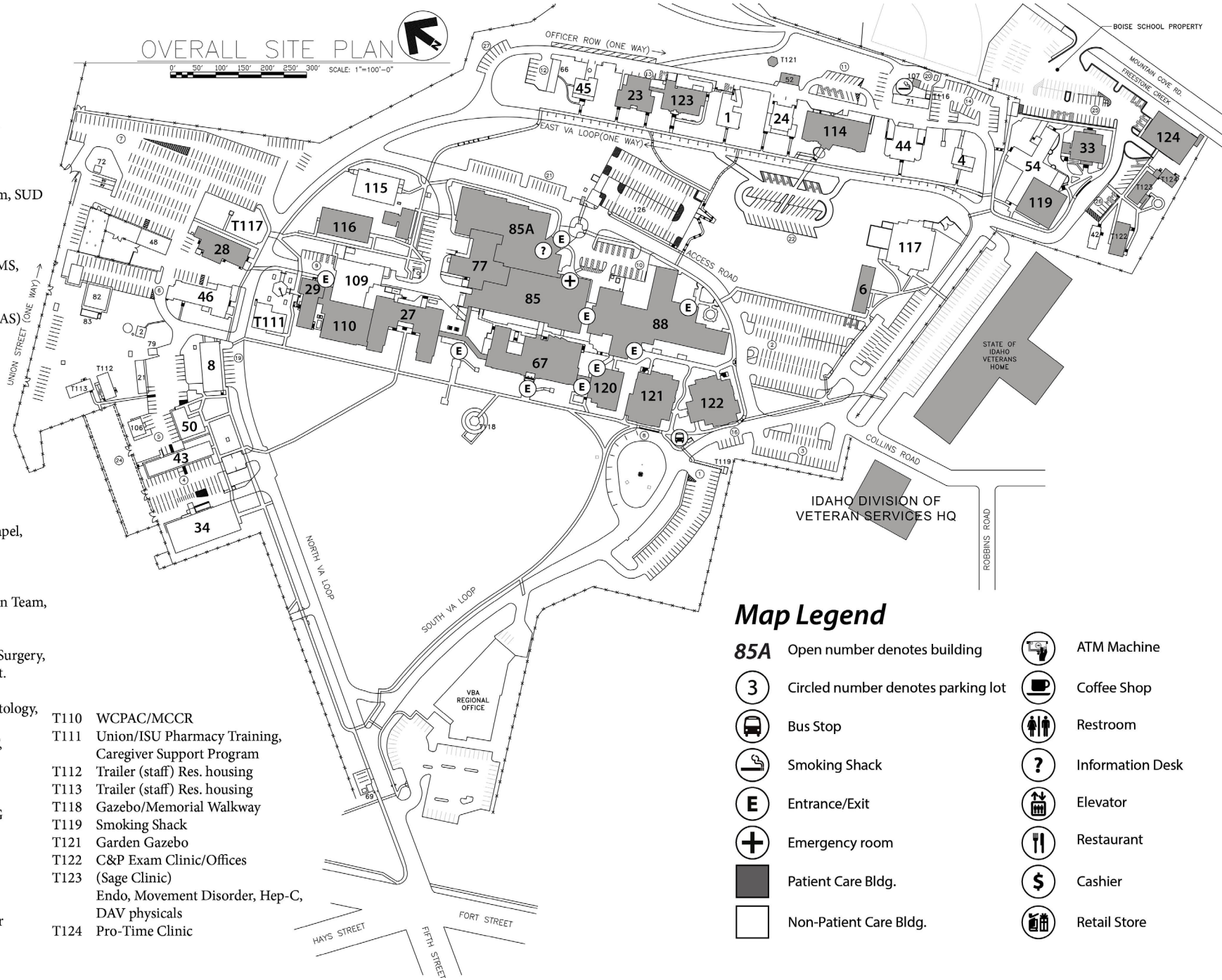
_____

Volunteer signature and date

Revised 2/22/2018

Bldg. # - Purpose/Activity/Service

1	Safety/GEMS/Emergency Mngmt.
4	Tele-Health
6	Eye Clinic/Optician
8	Shops/Student Housing
23	Recreation Therapy, CWT program, SUD Specialty Care
24	Human Resources Bldg.
27	(Inpatient/Outpatient Care) Oncology, Respiratory Therapy, 2MS, Prosthetics, Recreational Therapy.
29	Learning Resource Center (LRC)
33	Health Administration Service (HAS) & Non-VA Care Billing
34	Logistics
42	Tele-Health Hub
43	Print shop
44	Directors Office/Quality Dept.
45	Center of Excellence Offices
50	FMS Offices
52	Garden Pavilion
54	Education Bldg.
66	Storage
67	(Inpatient/Outpatient Care) Pain Clinic, Patient Advocate, Chapel, Police, Records, SDU.
77	Canteen
85	(Inpatient/Outpatient Care) ER/Admitting, Purple Team, Green Team, Travel, Radiology, Dental, ICU.
85A	(Outpatient/Specialty Care) Blue Team, Silver Team, Urology, Surgery, Laboratory, Pharmacy, Enrollment.
88	(Outpatient Care) Gold Team, Orange Team, Dermatology, Occupational Health.
110	Physical Therapy, Audiology, ENT, Peri-Operative Care, EMG
114	Behavioral Health Bldg.
115	Clinical Offices
116	Sleep Lab/Wellness Recovery, EEG
117	Research Bldg.
119	Gymnasium
120	MRI, Caregiver Support Program
121	Community Living Center (CLC)
122	Community Living Center (CLC)
123	Transformational Recovery Center
124	Women's Clinic



T110	WCPAC/MCCR
T111	Union/ISU Pharmacy Training, Caregiver Support Program
T112	Trailer (staff) Res. housing
T113	Trailer (staff) Res. housing
T118	Gazebo/Memorial Walkway
T119	Smoking Shack
T121	Garden Gazebo
T122	C&P Exam Clinic/Offices
T123	(Sage Clinic) Endo, Movement Disorder, Hep-C, DAV physicals
T124	Pro-Time Clinic

VA | U.S. Department of Veterans Affairs

OMB Number 2900-0090
Estimated Average: 15 min.

APPLICATION FOR VOLUNTARY SERVICE

The Paperwork Reduction Act of 1995 requires us to notify you that this information collection is in accordance with the clearance requirements of section 3507 of the Paperwork Reduction Act of 1995. We may not conduct or sponsor, and you are not required to respond to a collection of information unless it displays a valid OMB number. We anticipate that the time expended by all individuals who must complete this form will average 15 minutes. This includes the time it will take to read instructions, gather the necessary facts and fill out the form. The form is used to assist personnel of both voluntary organizations, which recruit volunteers from their membership, and the VA in the selection, screening and placement of volunteers in the nationwide VA Voluntary Service program. The volunteer program supplements the medical care and treatment of Veteran patients in all VA facilities.

PRIVACY ACT INFORMATION: The information requested on this form is solicited under the authority of 38 U.S.C. 7405(a)(1)(D) and will be used in the selection and placement of potential volunteers in the VA Voluntary Service Program. The information you supply may be disclosed outside VA as permitted by law; possible disclosures include those described in the 'routine uses' identified in the VA system of records 57VA135 Voluntary Service Records-VA, published in the Federal Register in accordance with the Privacy Act of 1974. The routine uses include disclosures: in response to court subpoenas, to report apparent law violations to other Federal, State or local agencies charged with law enforcement responsibilities, to service organizations, employers and Unemployment Compensation Offices to confirm volunteer service, and to congressional offices at the request of the volunteer. Disclosure of the information is voluntary, however, failure to furnish the information will hamper our ability to arrange the most satisfactory assignment for you and the Department of Veterans Affairs.

NAME (Last, First, Middle Initial)

ADDRESS (Street, City, State and Zip Code)

DATE

DATE OF BIRTH

TELEPHONE NUMBER

E-MAIL ADDRESS

SEX ☐ M ☐ F

ORGANIZATION MEMBERSHIP(S) (Unit, Post, Chapter, if Affiliated)

ASSIGNMENT PREFERENCES 1. 2. 3.

EXPERIENCE AND TRAINING (Special Skills/Abilities)

RESTRICTIONS, LIMITATIONS OF SERVICE (Health Concerns, Medications, Allergies, etc.)

AVAILABILITY (Days and Times)

IN CASE OF EMERGENCY, PLEASE CONTACT (Name, Relationship, Phone Number)

Monetary Waiver: I hereby waive all claims to monetary benefits for services rendered as a volunteer worker on a "without compensation basis" for an indefinite period. I understand that this waiver applies only to remuneration (compensation) for specific services rendered in the VA Voluntary Service (VAVS) Program and is not related to any other VA services or benefits to which I may be entitled. (**NOTE:** VA has entered into this agreement by the authority of 38 U.S.C. 7405(a)(1)(D). This agreement may be canceled by either party upon written notice.) I hereby accept the volunteer appointment(s) as outlined above.

Volunteer Signature

Date

I hereby appoint this applicant as a VA without-compensation employee subject to the provisions on this application. The above individual has been provided basic and assignment specific orientations which have been documented in the official volunteer folder located in the VA Voluntary Service Office.

VAVS Program Manager - Appointing Official Signature

Date

OFFICE USE ONLY

1. SUPERVISOR

2. SUPERVISOR PHONE NUMBER

3. ORIENTATIONS

4. UNIFORM

COMMENTS

NAME AND TITLE OF REVIEWER

DATE

EXISTING STOCK OF VA FORM 10-7055, MAY 2007, WILL BE USED.

To access the training manual, log on to the following web site:

http://www.boise.va.gov/giving/index.asp

Scroll down to where it says VA Voluntary Service Orientation Booklet. Click on the downloadable version of the Volunteer Orientation Booklet. Questions are located in the back of each training module in the book. Fill out the answer sheet front and back. Mark the answer that most accurately answers the question.

ORIENTATION ANSWER SHEET

DATE: _____

NAME: (Print) _____

SERVICE: _____**Voluntary**_____

YOUR POSITION:_____**Volunteer**_____

PAPER & PENCIL MODULES:

Circle the one correct answer

Prevention of Sexual Harassment

Q1	A	B		
Q2	A	B		
Q3	A	B		
Q4	A	B		
Q5	A	B		
Q6	A	B		
Q7	A	B		
Q8	A	B		
Q9	A	B	C	D
Q10	A	B	C	D

Ethics Awareness

Q1	A	B
Q2	A	B
Q3	A	B
Q4	A	B
Q5	A	B
Q6	A	B
Q7	A	B
Q8	A	B

Compliance & Business Integrity

Q1	A	B	C	D
Q2	A	B		
Q3	A	B	C	D
Q4	A	B	C	D
Q5	A	B		

General Safety

Q1	A	B		
Q2	A	B	C	D
Q3	A	B	C	D
Q4	A	B	C	D
Q5	A	B	C	D

Hazardous Materials

Q1	A	B	C	D
Q2	A	B	C	D
Q3	A	B		
Q4	A	B	C	D
Q5	A	B		
Q6	A	B	C	D

Life Safety/Fire Safety

Q1	A	B	C	D
Q2	A	B	C	D
Q3	A	B	C	D
Q4	A	B		
Q5	A	B	C	D

Medical Equipment

Q1	A	B	C	D
Q2	A	B	C	D
Q3	A	B	C	D
Q4	A	B		

Utilities

Q1	A	B	C	D
Q2	A	B		
Q3	A	B		
Q4	A	B	C	D
Q5	A	B	C	D

Emergency Preparedness

Q1	A	B	C	D
Q2	A	B	C	D
Q3	A	B		
Q4	A	B		
Q5	A	B	C	D

(OVER)

Infection Control

Q1	A	B	C	D
Q2	A	B		
Q3	A	B		
Q4	A	B		
Q5	A	B		
Q6	A	B	C	D

Drug Free Workplace

Q1	A	B	C	D
Q2	A	B		
Q3	A	B		
Q4	A	B	C	D

Prevention of Patient Abuse

Q1	A	B		
Q2	A	B		
Q3	A	B	C	D
Q4	A	B	C	D
Q5	A	B	C	D

Prevention of Violence in the Workplace

Q1	A	B	C	D
Q2	A	B		
Q3	A	B	C	D
Q4	A	B		
Q5	A	B		
Q6	A	B	C	D

Patient Safety

Q1	A	B			
Q2	A	B	C	D	
Q3	A	B			
Q4	A	B	C	D	
Q5	A	B	C	D	E

Age Specific Competencies

Q1	A	B
Q2	A	B
Q3	A	B
Q4	A	B
Q5	A	B

Security

Q1	A	B	C	D
Q2	A	B	C	D
Q3	A	B		
Q4	A	B		
Q5	A	B	C	D

Women Veterans Program

Q1	A	B
Q2	A	B
Q3	A	B
Q4	A	B
Q5	A	B
Q6	A	B

VA Privacy and Information Security Awareness and Rules of Behavior for Volunteers

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including VA sensitive information, or information systems of the U.S. Department of Veterans Affairs.

1. GENERAL RULES OF BEHAVIOR

a. I understand that an essential aspect of my job is to take personal responsibility for the secure use of VA systems and the VA data that it contains or that may be accessed through it, as well as the security and protection of VA information in any form (e.g., digital, paper).

b. I understand that when I use any government information system, I have NO expectation of privacy in any records that I create or in my activities while accessing or using such information system.

c. I understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. Authorized VA personnel include my supervisory chain of command as well as VA system administrators and ISOs. Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized OIG, VA, and law enforcement personnel.

d. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting of information on VA systems, modifying VA systems, unauthorized denying or granting access to VA systems, using VA resources for unauthorized use on VA systems, or otherwise misusing VA systems or resources. I also understand that attempting to engage in any of these unauthorized actions is also prohibited.

e. I understand that such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal or civil penalties. Depending on the severity of the violation, disciplinary or adverse action consequences may include: suspension of access privileges, reprimand, suspension from work, demotion, or removal. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may also result in criminal sanctions.

f. I understand that I have a responsibility to report suspected or identified information security incidents (security and privacy) to my VA supervisor, ISO and PO, immediately upon suspicion.

g. I understand that I have a duty to report information about actual or possible criminal violations involving VA programs, operations, facilities, contracts or information systems to my VA supervisor, local CIO and ISO, any management official or directly to the OIG, including reporting to the OIG Hotline. I also understand that I have a duty to immediately report to the OIG any possible criminal matters involving felonies, including crimes involving information systems.

h. I understand that the VA National ROB do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the U.S. Government.

i. I understand that the VA National ROB do not supersede any policies of VA facilities and other agency components that provide higher levels of protection to VA's information or information systems. The VA National ROB provide the minimal rules with which individual users must comply.

j. I understand that if I refuse to sign this VA National ROB as required by VA policy, I will be

denied access to VA information systems or VA sensitive information. Any refusal to sign the VA National ROB may have an adverse impact on my employment with the Department.

2. SPECIFIC RULES OF BEHAVIOR

a. Basic

(1) I will follow established VA information security and privacy policies and procedures.

(2) I will comply with any directions from my supervisors, VA system administrators, and ISOs concerning my access to, and use of, VA information and information systems or matters covered by these ROB.

(3) I understand that I may need to sign a non-VA entity's ROB to obtain access to their system in order to conduct VA business. While using their system, I must comply with their ROB. However, I must also comply with VA's National ROB whenever I am accessing VA information systems or VA sensitive information.

(4) I may be required to acknowledge or sign additional specific or unique ROB in order to access or use specific VA systems. I understand that those specific ROB may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.

b. Data Protection

(1) I will safeguard electronic VA sensitive information at work and remotely. I understand that all VA owned mobile devices must be encrypted using FIPS 140-2, Security Requirements for Cryptographic Modules, validated encryption (or its successor) unless encryption is not technically possible, as determined and approved by my local ISO, CIO and the DAS for OIS. This includes laptops, thumb drives, and other removable storage devices and storage media (e.g., CDs, Digital Video Discs (DVD).

(2) I understand that per VA Directive 6609, Mailing of Sensitive Personal Information, the following types of information are excluded from the encryption requirement when mailed according to the requirements outlined in the directive:

(a) Information containing the SPI of a single individual to:

1. That person (e.g., the Veteran's, beneficiary's, dependent's, or employee's own information) or to that person's legal representative (e.g., guardian, attorney-in-fact, attorney, or Veteran Service Organization). Such information may be mailed to an entity, not otherwise the subject of an exception, with the express written consent of the individual. Such information may be mailed via U.S. Postal Service regular mail unless tracked delivery service is requested and paid for by the recipient;

2. A business partner such as a health plan or insurance company, after reviewing potential risk;

3. A court, adjudicative body, parties in litigation, or to persons or entities in the course of a judicial or administrative proceeding; and

4. Congress, law enforcement agencies, and other governmental entities.

(b) Information containing SPI of one or more individuals to a person or entity that does not have the capability to decrypt information that is encrypted by VA, when sent according to VA Directive 6609.

(3) I understand that I must have approval from my supervisor to use, process, store, or transmit electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), regional offices).

(4) If approved to use, process, store, or transmit electronic VA sensitive information remotely, I must ensure any device I utilize is encrypted using FIPS 140-2 (or its successor) validated encryption. Information systems must use VA's approved configuration and security control requirements. The local CIO and ISO must reviewand approve (in writing) the mechanisms used to transport and store the VA sensitive data before it can be removed from the VA facility.

(5) I will ensure that all printouts of VA sensitive information that I work with, as part of my official duties, are physically secured when not in use (e.g., locked cabinet, locked door).

(6) I acknowledge that particular care should be taken to protect SPI aggregated in lists, databases, or logbooks, and will include only the minimum necessary SPI to perform a legitimate business function.

(7) I recognize that access to certain databases, regional-, or national-level data such as data warehouses or registries containing patient or benefit information, and data from other Federal agencies such as the Centers for Medicare and Medicaid or the Social Security Administration, has the potential to cause great risk to VA, its customers and employees due to the number and/or sensitivity of the records being accessed. I will act accordingly to ensure the confidentiality and security of these data commensurate with this increased potential risk.

(8) If I have been approved by my supervisor to take printouts of VA sensitive information home or to another remote location outside of a VA facility, or if I have been provided the ability to print VA sensitive information from a remote location to a location outside of a VA facility, I must ensure that the printouts are destroyed to meet VA disposal requirements when they are no longer needed and in accordance with all relevant records retention requirements. Two secure options that can be used are to utilize a shredder that meets VA and NIST's requirements or return the printouts to a VA facility for appropriate destruction.

(9) When in an uncontrolled environment (e.g., public access work area, airport, or hotel), I will protect against disclosure of VA sensitive information which could occur by eavesdropping, overhearing, or overlooking (shoulder surfing) from unauthorized persons. I will also follow a clear desk policy that requires me to remove VA sensitive information from view when not in use (e.g., on desks, printers, fax machines, etc.). I will also secure mobile and portable computing devices (e.g., laptops, USB thumb drives, PDA).

(10) I will use VA approved encryption to encrypt any e-mail, including attachments to the e-mail that contains VA sensitive information before sending the e-mail. I will not send any e-mail that contains VA sensitive information in an unencrypted form. I will not encrypt e-mail that does not include VA sensitive information or any e-mail excluded from the encryption requirement under para. b(2).

(11) I will not auto-forward e-mail messages to addresses outside the VA network.

(12) I will take reasonable steps to ensure fax transmissions are sent to the appropriate destination, including double checking the fax number, confirming delivery of the fax, using a fax cover sheet with the required notification message included and only transmitting individually

identifiable-information via fax when no other reasonable means exist and when someone is at the machine to receive the transmission or the receiving machine is in a secured location.

(13) I will protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by VA to protect sensitive data. I will only provide access to sensitive information to those who have a need-to-know for their professional duties, including only posting sensitive information to web-based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place for sensitive information. For questions regarding need-to-know and safeguards, I will obtain guidance from my VA supervisor, local CIO, and/or ISO before providing any access.

(14) When using wireless connections for VA business I will only use VA authorized wireless connections and will not transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140-2 (or its successor) validatedencryption.

(15) I will properly dispose of VA sensitive information, either in hardcopy, softcopy, or electronic format, in accordance with VA policy and procedures.

(16) I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized OIT employee.

c. Logical Access Controls

(1) I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor, local CIO, and/or ISO when the access is no longer needed.

(2) I will only utilize passwords that meet the VA minimum requirements defined in control **IA-5: Authenticator Management** in VA Handbook 6500, Appendix F, including using compliant passwords for authorized web-based collaboration tools that may not enforce such requirements.

(3) I will protect my verify codes and passwords from unauthorized use and disclosure. I will not divulge a personal username, password, access code, verify code, or other access requirement to anyone.

(4) I will not store my passwords or verify codes in any file on any IT system, unless that file has been encrypted using FIPS 140-2 (or its successor) validated encryption and I am the only person who can decrypt the file. I will not hardcode credentials into scripts or programs.

(5) I will use elevated privileges (e.g., Administrator accounts), if provided for the performance of my official duties, only when such privileges are needed to carry out specifically assigned tasks which require elevated access. When performing general user responsibilities, I will use my individual user account.

d. Remote Access/Teleworking

(1) I understand that remote access is allowed from other Federal Government computers and systems to VA information systems, subject to the terms of VA and the host Federal agency's policies.

(2) I agree that I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA-approved remote access software and services. I will use VA-provided IT equipment for remote access when possible.

(3) I agree that I will not have both a VA network connection and any non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by my VA supervisor, local CIO, and ISO.

(4) I am responsible for the security of VA property and information, regardless of my work location. VA security policies are the same and will be enforced at the same rigorous level when I telework as when I am in the office. I will keep government furnished equipment (GFE) and VA information safe, secure, and separated from my personal property and information.

(5) I will ensure that VA sensitive information, in any format, and devices, systems and/or software that contain such information or that I use to access VA sensitive information or information systems are adequately secured in remote locations (e.g., at home and during travel) and agree to periodic VA inspections of the devices, systems or software from which I conduct access from remote locations. I agree that if I work from a remote location, pursuant to an approved telework agreement with VA sensitive information, authorized OIT personnel may periodically inspect the remote location for compliance with required security requirements.

(6) I will protect information about remote access mechanisms from unauthorized use and disclosure.

(7) I will notify my VA supervisor, local CIO and ISO prior to any international travel with a mobile device (laptop, PDA) so that appropriate actions can be taken prior to my departure and upon my return, including potentially issuing a specifically configured device for international travel and/or inspecting the device or reimaging the hard drive upon return.

(8) I will exercise a higher level of awareness in protecting mobile devices when traveling internationally as laws and individual rights vary by country and threats against Federal employee devices may be heightened.

e. Non-VA Owned Systems

(1) I agree that I will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and approved in writing in advance by my VA supervisor, local CIO, and ISO. I agree that I will not access, transmit, or store remotely any VA sensitive information that is not encrypted using VA approved encryption.

(2) I will only use VA approved solutions for connecting non-VA owned systems to VA's network.

(3) I will obtain my local CIO's approval prior to connecting any non-VA equipment to VA's network at a VA facility. This includes directly connecting to a network port or utilizing remote access capabilities within the VA facility.

f. System Security Controls

(1) I will not attempt to override, circumvent, or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized VA staff. I will not attempt to alter the security configuration of government equipment unless authorized.

(2) I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA on VA equipment.

(3) I will not disable or degrade software programs used by VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information

systems, or to create, store or use VA information.

(4) I agree to have issued GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon demand.

(5) I will permit only those authorized by OIT to perform maintenance on IT components, including installation or removal of hardware or software.

g. System Access

(1) I will use only VA approved devices, systems, software, services, and data which I am authorized to use, including complying with any software licensing or copyright restrictions.

(2) I will only use VA approved collaboration technologies for conducting VA business.

(3) I will not download software from the Internet, or other public available sources, offered as free trials, shareware, or other unlicensed software to a VA owned system.

(4) I will not host, set up, administer, or operate any type of Internet server or wireless access point on any VA network unless explicitly authorized in writing by my local CIO and approved by my ISO. I will ensure that all such activity is in compliance with Federal and VA policies.

(5) I will not attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data.

(6) I will only use my access to VA computer systems and/or records for officially authorized and assigned duties. The use must not violate any VA policy regarding jurisdiction, restrictions, limitations or areas of responsibility.

(7) I will use my access under VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*, understanding that this Directive does not pertain to accessing VA applications or records. I will not engage in any activity that is prohibited by the Directive.

(8) I will prevent unauthorized access by another user by ensuring that I log off or lock any VA computer or console before walking away or initiate a comparable application feature that will keep others from accessing the information and resources available in my computing session.

h. Miscellaneous

(1) I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional role-based security training required, based on my roles and responsibilities.

(2) I will take precautions as directed by communications from my ISO and local OIT staff to protect my computer from emerging threats.

(3) I understand that while logged into authorized Web-based collaboration tools I am a representative of VA and I will abide by the ROB and all other policies and procedures related to these tools.

(4) I will protect government property from theft, loss, destruction, or misuse. I will follow VA policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for VA activities.

PRIVACY AND HIPAA FOCUSED TRAINING

Welcome and Introduction

Audience

All volunteers with direct access to protected health information (PHI) or access to PHI through VA computer systems are required to complete this training annually on the anniversary date of which they took the training the previous year.

All new employees with direct access to PHI or access to PHI through VA 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 created this training.

Goals

The goal of this training is to provide knowledge of:

Module 1

Basic Privacy Statutes and Employee Responsibilities

Module 2

Veterans 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)

Module 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, 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.

The Privacy Act (PA), 5 U.S.C. 552A – "The Privacy Act of 1974 (PA)," makes records of the Department of Veterans Affairs (VA) that are records about a living Individual who is a United States citizen or an alien lawfully admitted to US residence confidential.

Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulation the HIPAA Privacy Rule – 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.

Health Information Technology for Economic and Clinical Health (HITECH) Act – 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.

38 U.S.C. § 5701 Confidentiality Nature of Claims – 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.

38 U.S.C. § 5705 Confidentiality of Healthcare Quality Assurance Review Records – 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.

38 U.S.C. § 5701 Confidentiality of Certain Medical Records – 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.

The Freedom of Information Act (FOIA), 5 U.S.C. 552 – 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

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 ability to access PHI **does not** constitute authority to use PHI without a need to know.

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.

There is **NO** authority for an employee to access another employee's or a Veteran's health record unless it is in performance of their official job duties and it is for treatment, payment or health care operations. Appropriate disciplinary action may be taken by the supervisor with guidance from Human Resources.

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.

Privacy / FOIA Officer
500 West Fort Street (136)
Boise, ID 83702
(p) 208-422-1031
(f) 208-422-1592
Email: boiprivacyofficers@va.gov

Module 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,
Accounting of Disclosures,
Confidential Communications,
Request restriction of use or disclosure of records, and
File a complaint

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

IMPORTANT: 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 "Notice of Privacy Practices" (NoPP).

All newly registered Veterans receive a Notice of Privacy Practices by the Health Eligibility Center (HEC) at enrollment and at treatment for non-Veterans. 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 can be obtained from the Privacy Officer.

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. 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 for processing.

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 is pursuant to a FOIA request.

Entry of a VA patient by name or other identifier into a State Prescription Drug Monitoring database 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. Contact your VHA facility Chief of HIM and your local Privacy Officer for additional guidance.

When electronic batch reporting is available, it will capture the accounting of disclosure requirements, therefore eliminating the need for a note in CPRS or a manual accounting.

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,
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 not be allowed.

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, volunteers are 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, or
The U.S. Department of Health and Human Services, Office for Civil Rights

Module 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 about:

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 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, an additional VA Form 10-3203 *Consent for Use of Picture and/or Voice* is required.

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; and

Reducing the use of the SSN whenever possible.

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 may be 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 Health 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 heath care facility Privacy Officer.

Module 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.

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, if requesting 7332 protected information, the request must specifically state that

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.

VHA will request individuals to respect the privacy of patients and others if they want to take photographs or capture digital images and video/audio recordings on VHA premises.

NOTE: Secretly taking pictures or recording conversations is strongly discouraged.

Module 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
Compliance
Virtual Lifetime Electronic Record (VLER)

Release of U.S.C. §7332 Protected Health Information

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.
The following is a list of situations where 38 U.S.C. § 7332 protected information **CAN** be released without a signed authorization:

To medical personnel to the extent necessary to meet a bona fide medical emergency;

To qualified personnel for conducting scientific research, management audits, financial audits or program evaluations;

To public health authority charged under federal or state law for protection of public health pursuant to a standing written request; or

To a court of competent jurisdiction pursuant to a **very specific** Court Order.

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 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 All requests for logbooks are processed by the facility Privacy Officer. 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 volunteers 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.

Compliance

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

Employees who have access to VHA records or VHA computer systems shall be instructed on an ongoing basis about the requirements of Federal privacy and information laws, regulations, VA and VHA policy. Employees' access or use of PHI is limited to the minimum necessary standard of information needed to perform their official job duties. See VHA Handbook 1605.02, "Minimum Necessary Standards for Protected Health Information" for additional guidance.

The Omnibus final rule imposes a tiered penalty structure and the penalties imposed vary based on the severity of the violation. The penalties range from $100 to $50,000 per violation, with a $1.5 million cap per calendar year for multiple violations of identical provisions, and criminal penalties of up to 10 years' imprisonment.

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).

Module 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.

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)

This concludes the Privacy and HIPAA Focused Training for FY2017.

Certificate of Completion
Privacy and HIPAA Training
&
Rules of Behavior Certificate of Completion

I, _____ certify that I have completed the Privacy and HIPAA training. I acknowledge that I have received a copy of the Rules of Behavior and understand, accept and agree to comply with all terms and conditions of the Rules of Behavior.

_____
Signature of Volunteer and date

_____
Signature of Staff and date

VOLUNTARY SERVICE DRESS CODE

1. Do wear clean, neat clothing. Pants must be secured around the waist. Underwear should not be displayed as part of the outer dress.

2. Do observe proper hygiene.

3. Do wear comfortable shoes with good support. If volunteering in patient areas, wear closed toed shoes (for example: tennis, track, etc.) Do not wear flip-flops or open toed shoes.

4. Do not wear shorts, pants that are frayed or have holes in them, shirts that reveal cleavage or expose the midriff.

5. Body piercings will not be worn while at work. If you have eyebrow, nose, lip or tongue piercings they must be removed while on duty.

6. Do not wear perfume or cologne while working in the hospital.

7. Bermuda shorts may be worn if your assignment is out doors or driving.

8. When in doubt, please **ASK**.

9. I have read the dress code and plan to observe it.

_____ _____

Signature Date

Declaration for Federal Employment*

(*This form may also be used to assess fitness for federal contract employment)

Form Approved:
OMB No. 3206-0182

Instructions

The information collected on this form is used to determine your acceptability for Federal and Federal contract employment and your enrollment status in the Government's Life Insurance program. You may be asked to complete this form at any time during the hiring process. Follow instructions that the agency provides. If you are selected, before you are appointed you will be asked to update your responses on this form and on other materials submitted during the application process and then to recertify that your answers are true.

All your answers must be truthful and complete. **A false statement on any part of this declaration or attached forms or sheets may be grounds for not hiring you, or for firing you after you begin work. Also, you may be punished by a fine or imprisonment (U.S. Code, title 18, section 1001).**

Either type your responses on this form or print clearly in dark ink. If you need additional space, attach letter-size sheets (8.5" X 11"). Include your name, Social Security Number, and item number on each sheet. We recommend that you keep a photocopy of your completed form for your records.

Privacy Act Statement

The Office of Personnel Management is authorized to request this information under sections 1302, 3301, 3304, 3328, and 8716 of title 5, U. S. Code. Section 1104 of title 5 allows the Office of Personnel Management to delegate personnel management functions to other Federal agencies. If necessary, and usually in conjunction with another form or forms, this form may be used in conducting an investigation to determine your suitability or your ability to hold a security clearance, and it may be disclosed to authorized officials making similar, subsequent determinations.

Your Social Security Number (SSN) is needed to keep our records accurate, because other people may have the same name and birth date. Public Law 104-134 (April 26, 1996) asks Federal agencies to use this number to help identify individuals in agency records. Giving us your SSN or any other information is voluntary. However, if you do not give us your SSN or any other information requested, we cannot process your application. Incomplete addresses and ZIP Codes may also slow processing.

ROUTINE USES: Any disclosure of this record or information in this record is in accordance with routine uses found in System Notice OPM/GOVT-1, General Personnel Records. This system allows disclosure of information to: training facilities; organizations deciding claims for retirement, insurance, unemployment, or health benefits; officials in litigation or administrative proceedings where the Government is a party; law enforcement agencies concerning a violation of law or regulation; Federal agencies for statistical reports and studies; officials of labor organizations recognized by law in connection with representation of employees; Federal agencies or other sources requesting information for Federal agencies in connection with hiring or retaining, security clearance, security or suitability investigations, classifying jobs, contracting, or issuing licenses, grants, or other benefits; public and private organizations, including news media, which grant or publicize employee recognitions and awards; the Merit Systems Protection Board, the Office of Special Counsel, the Equal Employment Opportunity Commission, the Federal Labor Relations Authority, the National Archives and Records Administration, and Congressional offices in connection with their official functions; prospective non-Federal employers concerning tenure of employment, civil service status, length of service, and the date and nature of action for separation as shown on the SF 50 (or authorized exception) of a specifically identified individual; requesting organizations or individuals concerning the home address and other relevant information on those who might have contracted an illness or been exposed to a health hazard; authorized Federal and non-Federal agencies for use in computer matching; spouses or dependent children asking whether the employee has changed from a self-and-family to a self-only health benefits enrollment; individuals working on a contract, service, grant, cooperative agreement, or job for the Federal government; non-agency members of an agency's performance or other panel; and agency-appointed representatives of employees concerning information issued to the employees about fitness-for-duty or agency-filed disability retirement procedures.

Public Burden Statement

Public burden reporting for this collection of information is estimated to vary from 5 to 30 minutes with an average of 15 minutes per response, including time for reviewing instructions, searching existing data sources, gathering the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden, to the U.S. Office of Personnel Management, Reports and Forms Manager (3206-0182), Washington, DC 20415-7900. The OMB number, 3206-0182, is valid. OPM may not collect this information, and you are not required to respond, unless this number is displayed.

Declaration for Federal Employment*

Form Approved:
OMB No. 3206-0182

(*This form may also be used to assess fitness for federal contract employment)

GENERAL INFORMATION

1. **FULL NAME** (Provide your full name. If you have only initials in your name, provide them and indicate "Initial only". If you do not have a middle name, indicate "No Middle Name". If you are a "Jr.," "Sr.," etc. enter this under Suffix. First, Middle, Last, Suffix)

♦

2. **SOCIAL SECURITY NUMBER**

♦

3a. **PLACE OF BIRTH** (Include city and state or country)

♦

3b. **ARE YOU A U.S. CITIZEN?**

☐ YES ☐ NO (If "NO", provide country of citizenship) ♦

4. **DATE OF BIRTH** (MM / DD / YYYY)

♦

5. **OTHER NAMES EVER USED** (For example, maiden name, nickname, etc)

♦

♦

6. **PHONE NUMBERS** (Include area codes)

Day ♦

Night ♦

Selective Service Registration

If you are a male born after December 31, 1959, and are at least 18 years of age, civil service employment law (5 U.S.C. 3328) requires that you must register with the Selective Service System, unless you meet certain exemptions.

7a. Are you a male born after December 31, 1959? ☐ YES ☐ NO (If "NO", proceed to 8.)

7b. Have you registered with the Selective Service System? ☐ YES (If "YES", proceed to 8.) ☐ NO (If "NO", proceed to 7c.)

7c. If "NO," describe your reason(s) in item 16.

Military Service

8. Have you ever served in the United States military? ☐ YES (If "YES", provide information below) ☐ NO

If you answered "YES," list the branch, dates, and type of discharge for all active duty.
If your only active duty was training in the Reserves or National Guard, answer "NO."

Branch	From (MM/DD/YYYY)	To (MM/DD/YYYY)	Type of Discharge

Background Information

For all questions, provide all additional requested information under item 16 or on attached sheets. The circumstances of each event you list will be considered. However, in most cases you can still be considered for Federal jobs.

For questions 9,10, and 11, your answers should include convictions resulting from a plea of *nolo contendere* (no contest), but omit (1) traffic fines of $300 or less, (2) any violation of law committed before your 16th birthday, (3) any violation of law committed before your 18th birthday if finally decided in juvenile court or under a Youth Offender law, (4) any conviction set aside under the Federal Youth Corrections Act or similar state law, and (5) any conviction for which the record was expunged under Federal or state law .

9. During the last 7 years, have you been convicted, been imprisoned, been on probation, or been on parole? (Includes felonies, firearms or explosives violations, misdemeanors, and all other offenses.) *If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved.* ☐ YES ☐ NO

10. Have you been convicted by a military court-martial in the past 7 years? *(If no military service, answer "NO.") If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the military authority or court involved.* ☐ YES ☐ NO

11. Are you currently under charges for any violation of law? *If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved.* ☐ YES ☐ NO

12. During the last 5 years, have you been fired from any job for any reason, did you quit after being told that you would be fired, did you leave any job by mutual agreement because of specific problems, or were you debarred from Federal employment by the Office of Personnel Management or any other Federal agency? *If "YES," use item 16 to provide the date, an explanation of the problem, reason for leaving, and the employer's name and address.* ☐ YES ☐ NO

13. Are you delinquent on any Federal debt? (Includes delinquencies arising from Federal taxes, loans, overpayment of benefits, and other debts to the U.S. Government, plus defaults of Federally guaranteed or insured loans such as student and home mortgage loans.) *If "YES," use item 16 to provide the type, length, and amount of the delinquency or default, and steps that you are taking to correct the error or repay the debt.* ☐ YES ☐ NO

Declaration for Federal Employment*

(*This form may also be used to assess fitness for federal contract employment)

Form Approved:
OMB No. 3206-0182

Additional Questions

14. Do any of your relatives work for the agency or government organization to which you are submitting this form? (Include: father, mother, husband, wife, son, daughter, brother, sister, uncle, aunt, first cousin, nephew, niece, father-in-law,mother-in-law, son-in-law, daughter-in-law, brother-in-law, sister-in-law, stepfather, stepmother, stepson, stepdaughter, stepbrother, stepsister, half brother, and half sister.) *If "YES," use item 16 to provide the relative's name,relationship, and the department, agency, or branch of the Armed Forces for which your relative works.* ☐ YES ☐ NO

15. Do you receive, or have you ever applied for, retirement pay, pension, or other retired pay based on military, Federal civilian, or District of Columbia Government service? ☐ YES ☐ NO

Continuation Space / Agency Optional Questions

16. Provide details requested in items 7 through 15 and 18c in the space below or on attached sheets. Be sure to identify attached sheets with your name, Social Security Number, and item number, and to include ZIP Codes in all addresses. If any questions are printed below, please answer as instructed *(these questions are specific to your position and your agency is authorized to ask them).*

Certifications / Additional Questions

APPLICANT: If you are applying for a position and have not yet been selected, carefully review your answers on this form and any attached sheets. When this form and all attached materials are accurate, read item 17, and complete 17a.

APPOINTEE: If you are being appointed, carefully review your answers on this form and any attached sheets, including any other application materials that your agency has attached to this form. If any information requires correction to be accurate as of the date you are signing, make changes on this form or the attachments and/or provide updated information on additional sheets, initialing and dating all changes and additions. When this form and all attached materials are accurate, read item 17, complete 17b, read 18, and answer 18a, 18b, and 18c as appropriate.

17. **I certify** that, to the best of my knowledge and belief, all of the information on and attached to this Declaration for Federal Employment, including any attached application materials, is true, correct, complete, and made in good faith . **I understand that a false or fraudulent answer to any question or item on any part of this declaration or its attachments may be grounds for not hiring me, or for firing me after I begin work, and may be punishable by fine or imprisonment. I understand** that any information I give may be investigated for purposes of determining eligibility for Federal employment as allowed by law or Presidential order. **I consent** to the release of information about my ability and fitness for Federal employment by employers, schools, law enforcement agencies, and other individuals and organizations to investigators, personnel specialists, and other authorized employees or representatives of the Federal Government. **I understand** that for financial or lending institutions, medical institutions, hospitals, health care professionals, and some other sources of information, a separate specific release may be needed, and I may be contacted for such a release at a later date.

17a. Applicant's Signature: _____ Date _____
(Sign in ink)

17b. Appointee's Signature: _____ Date _____
(Sign in ink)

Appointing Officer:
Enter Date of Appointment or Conversion
MM / DD / YYYY

18. **Appointee (Only respond if you have been employed by the Federal Government before):** Your elections of life insurance during previous Federal employment may affect your eligibility for life insurance during your new appointment. These questions are asked to help your personnel office make a correct determination.

18a. When did you leave your last Federal job? DATE: MM / DD / YYYY

18b. When you worked for the Federal Government the last time, did you waive Basic Life Insurance or any type of optional life insurance? ☐ YES ☐ NO ☐ DO NOT KNOW

18c. If you answered "YES" to item 18b, did you later cancel the waiver(s)? If your answer to item 18c is "NO," use item 16 to identify the type(s) of insurance for which waivers were not canceled. ☐ YES ☐ NO ☐ DO NOT KNOW

Form Approved: OMB No. 2900-0676
Respondent Burden: 5 Minutes

Department of Veterans Affairs

REQUEST FOR PERSONAL IDENTITY VERIFICATION CARD

PRIVACY ACT STATEMENT: VA is authorized to ask for the information requested on this form by Homeland Security Presidential Directive (HSPD)-12, and 31 USC 7701. The information and biometrics collected, collected as part of the Federal identity-proofing program under HSPD-12 are used to verify the personal identity of VA applicants for employment, employees, contractors, and affiliates (such as students, WOC employees, and others) prior to issuing a Department identification credential. The credentials themselves are to be used to authenticate electronic access requests from VA employees, contractors, and affiliates issued a Department identification credential to gain access to VA facilities and networks (where available) through digital access control systems, as well as to other federal government agency facilities and systems where permitted by law. The information collected on this form is protected by the Privacy Act, 5 USC Section 552(a) and maintained under the authority of 38 USC Section 501 and 38 USC Sections 901-905 in VA system of records "Police and Security Records-VA (103VA07B)". VA may make a "routine use" disclosure of the information in this system of records for the routine uses listed in this system of records, including: civil or criminal law enforcement, constituent congressional communications initiated at your request, litigation or administrative proceedings in which the United States is a party or has an interest, the administration of VA programs, verification of identity and status, and personnel administration by Federal agencies. Failure to provide all of the requested information may result in VA being unable to process your request for a Personal Identity Verifiction Card, or denial of issuance of a Personal Identity Verification Card. If you do not have a Personal Identity Verification Card, you may not be granted access to VA facilities or networks, which could have an adverse impact on your application to become, or status as, a VA employee, contractor or affiliate where such access is required to perform your assigned duties or responsibilities.

PAPERWORK REDUCTION ACT NOTICE: The public reporting burden is approximately 5 minutes including time to review instruction, find the information, and complete this form. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the VA Clearance Officer (005E3), 810 Vermont Avenue, Washington, DC 20420.

SECTION I - APPLICANT INFORMATION

APPLICANT INFORMATION *(Completed by Applicant)*

1. LEGAL NAME OF APPLICANT *(Insert last, first, middle and suffix name)*
2. NICKNAME TO BE USED FOR APPLICANT *(Insert last name and first name, if applicable)*
3. DATE OF BIRTH *(MM/DD/YYYY)*
4. SOCIAL SECURITY NO.
5. HOME PHONE NUMBER *(Include Area Code)* ***(Optional)***
6. HOME E-MAIL ADDRESS ***(Optional)***
7. HOME ADDRESS
8. SIGNATURE OF APPLICANT
9. DATE SIGNED

SECTION II - SPONSOR VERIFICATION *(Completed by Sponsor)*

PART A - APPLICANT EMPLOYMENT INFORMATION *(Completed by Sponsor)*

1. NAME AND ADDRESS OF FACILITY OR ASSIGNED DUTY STATION

Boise VAMC
500 W. Fort Street
Boise, ID 83702

2. NAME OF SPONSORING DEPARTMENT, SERVICE, OR SECTION, AND MAIL ROUTING SYMBOL
3. CREDENTIALS/ORGANIZATIONAL TITLE *(AKA Position/Job Title)*
4. COST CTR.
5. WORK PHONE NUMBER *(If applicable)*
6. WORK E-MAIL ADDRESS

PART B - TYPE OF REQUEST AND EMPLOYMENT STATUS *(Completed by Sponsor)*

1. TYPE OF REQUEST
☐ NEW ID ☐ RENEWAL ☐ REPLACEMENT ID *(Damaged/Lost)* ☐ CHANGE LEVEL OF ACCESS

2. TYPE OF CARD
☐ PERSONAL IDENTITY VERIFICATION (PIV) ☐ VA (NON-PIV)

3. TYPE OF ACCESS
☐ LOGICAL ACCESS _____ *(Domain)* ☐ PHYSICAL ACCESS *(Complete Part D)*

4. EMPLOYMENT STATUS
☐ VA EMPLOYEE ☐ CONTRACTOR ☐ AFFILIATE *(Specify)* ☐ TEMPORARY VA EMPLOYMENT

PART C - PHYSICAL SECURITY ACCESS DATA *(Completed by Sponsor)*

1. SPECIAL SECURITY ACCESS REQUIRED
☐ YES *(If "YES," Specify in Item2)* ☐ NO

2. SPECIFY LOCATION OF SPECIAL SECURITY *(i.e. tower, bldg. no., etc.)*

3. IS APPLICANT A KEY EMERGENCY RESPONDER, CRITICAL EMPLOYEE, OR NEITHER?
☐ EMERGENCY RESPONDER
☐ CRITICAL EMPLOYEE ☐ NEITHER

PART D - TYPE OF BACKGROUND INVESTIGATION FOR POSITION *(Completed by Sponsor)*

TYPE OF BACKGROUND INVESTIGATION FOR POSITION
☐ SAC ☐ NACI ☐ SECRET ☐ TOP SECRET ☐ OTHER *(Specify)*

PART E - CONTRACTORS, AFFILIATES, AND TEMPORARY EMPLOYMENT INFORMATION *(Completed by Sponsor)*

1. EMPLOYMENT EXPIRATION DATE /CONTRACT END DATE *(MM/DD/YYYY)(For Contractors, Affiliates, and Temporary Employment)*
2. NAME OF FIRM OR COMPANY *(If applicable)*
3. NAME OF CONTRACTING OFFICER TECH. REPR. *(If applicable)*
4. NAME OF RESPONSIBLE VA ORGANIZATION
5. MAIL ROUTING SYM.

PART F - SPONSOR AUTHORIZATION AND CERTIFICATION *(Completed by Sponsor)*

CERTIFICATION: I Certify under penalty of perjury that the information in Section II is true and correct.

1. NAME OF SPONSOR	2. SPONSOR CREDENTIALS/ORGANIZATIONAL TITLE	
3. CERTIFICATE NUMBER *(Issued by PCI Manager or Registrar)*	4. SIGNATURE OF SPONSOR	5. DATE SIGNED *(MM/DD/YYYY)*
6. WORK ADDRESS Boise VAMC 500 W Fort St. Boise, ID 83702	7. NAME OF SPONSOR'S DEPARTMENT, SERVICE, OR SECTION 8. WORK PHONE NUMBER *(Include Area Code)* 9. WORK E-MAIL ADDRESS	

SECTION III - APPLICANT IDENTITY VERIFICATION *(Completed by Registrar)*

INSTRUCTIONS: To be completed and signed by Registrar at the time of proofing. Review Section I - Applicant Information, and Section II - Sponsor Verification, assuring that information has been filled out correctly and signed accordingly. The identification must follow these guidelines:

- Applicant must present two (2) forms of identification from the Accepted Identification Documentation List.
- The names on the identification must match exactly (If one ID has a full middle name, and the other has a middle initial, then the initial must match).
- One State or Federal ID must contain a photograph. • Both IDs must be original documents. • Both IDs must be currently valid, not expired.
- Verify that the applicant has background informaition on file. If no evidence of a SAC exists, then capture fingerprint data and process accordingly.

PART A - BACKGROUND CHECK

1. TYPE OF BACKGROUND CHECK

	SAC *(Fingerprint Check)*	NACI	OTHER *(Specify)*
1A. DATE INITIATED BACKGROUND CHECK *(MM/DD/YYYY)*			
1B. DATE ADJUDICATED BACKGROUND CHECK *(MM/DD/YYYY)*			

2. FINGERPRINTS CAPTURE REQUIRED? ☐ YES ☐ NO *(If "NO," proceed to Part B)*	3. SEX	4. RACE	5. HEIGHT	6. WEIGHT	7. EYES	8. HAIR	9. PLACE OF BIRTH

10. NOTICABLE SCARS AND TATTOOS

PART B - PHOTOGRAPHIC IDENTIFICATION NUMBER 1

1. EXACT NAME LISTED ON PHOTO ID	2. DOCUMENT IDENTIFICATION NUMBER	3. EXPIRATION DATE *(MM/DD/YYYY)*
4. DOCUMENT TYPE	5. ISSUANCE DATE *(MM/DD/YYYY)*	6. ISSUING AUTHORITY

PART C - IDENTIFICATION NUMBER 2

1. EXACT NAME LISTED ON ID	2. DOCUMENT IDENTIFICATION NUMBER	3. EXPIRATION DATE *(MM/DD/YYYY)*
4. DOCUMENT TYPE	5. ISSUANCE DATE *(MM/DD/YYYY)*	6. ISSUING AUTHORITY

PART D - REGISTRAR INFORMATION AND SIGNATURE

1. WORK ADDRESS Boise VAMC 500 W Fort St. Boise, ID 83702	2. PRINTED NAME OF REGISTRAR 3. NAME OF DEPARTMENT, SERVICE, OR SECTION 4. WORK PHONE NUMBER *(Include Area Code)*	5. WORK E-MAIL ADDRESS
6. DATE APPLICANT INITIATED BACKGROUND INVESTIGATION	7. APPLICANT'S REQUEST FOR PERSONAL IDENTITY VERIFICATION CARD **ACTION TAKEN:** ☐ APPROVED ☐ DENIED	

CERTIFICATION: I certify that under penalty of perjury that I have examined the documents presented by the above named person, and that the above listed documents appear to be genuine and to relate to the person named.

8. SIGNATURE OF REGISTRAR	9. DATE SIGNED *(MM/DD/YYYY)*

AdobeFormsDesigner

Department of Veterans Affairs

Assignment of Functional Categories

Employee's Name:

Job Title: Volunteer

Department/Service Assigned:

An Assignment of Functional Category is a classification of an employee by their supervisor indicating their level of access to Individually Identifiable health Information (IIHI) and/or Protected Health Information (PHI). This form must be completed 1) upon hiring and in-processing; 2) annually thereafter; and 3) as needed due to job changes between annual reviews. Supervisor and employees should have a discussion which clearly communicates the level of access to IIHI/PHI as well as when, and what, employees may access in the performance of their assigned duties. Functional category for medical residents or other health professional trainees is assigned within their MTT training (TMS 3185966 or 3192008). If an employee's duties are covered by more than one functional category listed below, access should be granted based on the less restrictive category to meet the need of an intended purpose.

Immediate Supervisor: Check off functional category, review with employee, obtain signatures, and maintain copy in the *Supervisor's Personnel Files* (RCS10-1,3000.18) for the individual employee.

	Functional Categories (Class of Persons)	**Type of Protected Health Information Accessible**	**Allowable Systems of Records for Limited Access**	**Primary Conditions for Access to Information**
☐	Direct Care Providers (e.g., Doctor, Nurse, Psychologist, Pharmacist, Social Worker, Therapists, Dietitian)	Entire Health Record		Treatment of Individuals
☐	Department of Veterans Affairs (VA) Researchers	Entire Health Record including Research Records		Activities as approved by an Institutional Review Board or Privacy Board
☐	Indirect Care Providers (e.g., Pharmacy/Lab/X-ray Technicians)	Entire Health Record		In support of treatment of individuals
☐	Chief Business Office (CBO) Administrative	Entire Health Record		In support of CBO functions such as payment, reimbursement, income verification and eligibility benefits
☐	Health Information Support Services (e.g., Medical Support Assistants, Medical Record Administrators/ Technicians)	Entire Health Record		Assign diagnostic codes, transcribe, file, release information, scan, patient look up, provide or input health information or registry data
☐	Quality, Oversight and Investigations (e.g., Quality Management, Risk Manager, Infection Control Nurse, Utilization Reviewer, Patient Safety Officer)	Entire Health Record		Address medical inspections, investigations, complaint review and resolution,quality reviews,patient safety reviews,compliance reviews, and provide congressional responses
☐	Chief of Police, Assistant Chief of Police Officer	Limited Health Record	79VA10P2, 24VA10P2	Reviewing Patient Inquiry
☐	Police and Security Service	No Need for access to PHI		Security functions
☐	Information Security, Privacy, Compliance Officers, VISN Staff, Patient Advocate	Entire Health Record including Research Records		Monitoring and tracking of security, privacy, patient care and compliance issues

	Functional Categories (Class of Persons)	Type of Protected Health Information Accessible	Allowable Systems of Records for Limited Access	Primary Conditions for Access to Information
☐	Operations Support (Mail Room, Contracting, Acquisitions, Human Resources, Education, Library, Engineering, Radiation and Environmental Safety)	No need for access to PHI		Internal operations
☐	Facility and VISN Leadership and Management	Limited Health Record, where necessary to complete assignment	24VA10P2, 79VA10P2, 121VA10P2 and any other system of records with national data	Overseeing of operation and management, executive decisions for health care operations
☐	Non-Health Information Administrative Support (MHV Coordinator, Bio-Medical, Administrator Officer of the Day (AOD), Equal Employment Opportunity (EEO), Public Affairs, Call Center Support, Program Support Staff, Telecommunications)	Limited Health Record, where necessary to complete assignment	79VA10P2, 24VA10P2	Administrative, public, and employee support
☐	Environmental Support Staff (e.g. Groundskeepers, Building Management)	No need for access to PHI		Maintenance of grounds, buildings, and housekeeping
☐	Information Technology (e.g. Clinical Application Coordinators, OI&T Staff, Decision Support Staff, Chief Medical Information Officer, Chief Health Informatics Officer)	Limited Health Record, where necessary to complete assignment	79VA10P2, 24VA10P2, 121VA10P2 and any other system of records for an IT system.	Maintenance and support of computer systems
☐	Veterans Canteen Service, Cafeteria, Retail Store	No need for access to PHI		Retail and food services for employees and Veterans
☒	Volunteer Services (e.g., Reception Desk, Escorts, Transport Drivers)	Limited Health Record, where necessary to complete assignment	79VA10P2, 24VA10P2	Transportation and other services
☐	VHA Program Office, VACO leadership	Limited access where necessary to complete task	79VA10P2, 24VA10P2	To correspond to Congressional inquires and general correspondence inquires

Department of Veterans Affairs

Assignment of Functional Categories

Employee's Name:	Job Title: Volunteer
Department/Service Assigned:	

SIGNATURES

By signing this document, I acknowledge and understand that I have been assigned the functional categories listed above and given computer access and VistA menu options, if applicable, to access and use Protected Health Information only in the performance of my official job duties and assigned tasks. I will not access, use, or disclose Protected Health Information in any way that does not comply with the Minimum Necessary Standard for Use and Disclosure of Protected Health Information.

Employee's Signature:	Date:
Supervisor's Signature:	Date:

ANNUAL REVIEWS

Note: A new VA Form 10-0539 must be completed if any changes have been made to the functional category assignments or if there has been a change in duties. If no changes have been made, complete the bottom portion during the employee's annual performance appraisal review.

Employee's Signature:	Date:
Supervisor's Signature:	Date:
Employee's Signature:	Date:
Supervisor's Signature:	Date:
Employee's Signature:	Date:
Supervisor's Signature:	Date:
Employee's Signature:	Date:
Supervisor's Signature:	Date:
Employee's Signature:	Date:
Supervisor's Signature:	Date:
Employee's Signature:	Date:
Supervisor's Signature:	Date:
Employee's Signature:	Date:
Supervisor's Signature:	Date: