

**PLEASE READ THIS BEFORE
FILLING OUT YOUR APPLICATION**

1. In an effort to process your application for residency in a timely manner, and to prevent any delay in your practicing at the VA Medical Center, please be sure to fill in every category on the application form VA #10-2850D.
2. Please DO NOT print out application back to back
3. Regarding ECFMG certificates: We must have a copy of your valid certificate. It must be valid either thru the next academic year, or valid indefinitely. This **copy must be included when you send the application to us.**
4. **Also, there can be no gaps in time between the time you graduated Medical School and the time you begin your internship or residency. All the months and years must be accounted for on the application. If there is not enough space, please use a separate piece of paper and attach a copy of your CV.**
5. If a question or section doesn't apply to you, simply put "N/A". Do not leave anything blank. Yes or No questions need to be answered – do not leave blank.
6. Be sure to sign all the forms.
7. If you have a VISA, it must be valid through the next academic year. **A copy of your VISA must be included with your application.** If you were given an IAP-66 form for renewing your VISA, you must provide us with a copy of that. If you have a green card, you **must include a copy of both sides of your green card.** We need the form from immigration, not the stamp in your passport.
8. If you are a naturalized citizen, you must include with your application **a copy of your naturalization papers or a copy of your passport.**
9. You MUST provide an NPI (National Provider Identifier) number.
10. Please provide a current CV

NOTE: Your application will not be processed unless completed!!! Applications take at least 30 days to process; therefore you must have your application completed, in our office no later than 30 days prior to your scheduled rotation at the VA. **You can not practice medicine at the VA without your application signed off by the Facility Designated Education Officer or Designee.**

If you have any questions, feel free to contact Liz Castellon at 203-932-5711 ext 2704 or email Elizabeth.Castellon@va.gov

Please mail the application to

Liz Castellon
Dept of Medicine/111
950 Campbell Ave
West Haven, CT 06516



**DEPARTMENT OF VETERANS AFFAIRS
VA Connecticut Healthcare System
950 Campbell Avenue
West Haven, Connecticut 06510**

Dear

Welcome to the Department of Veterans Affairs. You will be assigned to our facility as _____ Woc Housestaff _____ from _____ through _____ under the authority of 38 U.S.C. 7406. During your period of affiliation with our facility, you are authorized to perform services as directed by the Chief of Medicine _____.

In accepting this assignment you will receive no monetary compensation and will not be entitled to those benefits normally given to regularly paid employees of the Veterans Health Administration, such as leave, retirement, etc. You will, however, be eligible to receive the benefits indicated below. Cash cannot be paid in lieu of any of these benefits.

- Quarters Subsistence Uniforms Laundering of Uniforms

If you agree to these conditions, please sign the statement below and return the letter in the enclosed postage-free envelope. This agreement may be terminated at any time by either party by written notice of such intent.

Please indicate your veteran status by circling the appropriate number below.

Sincerely yours,

Chief, Human Resources Management Service

Enclosure

I agree to serve in the above capacity under the conditions indicated.

Veteran Status

- 1-Vietnam Veteran*
- 2-Other Veteran
- 3-Non-Veteran

**For this purpose, a Vietnam Veteran is one with, service between August 5, 1964, and May 7, 1975.*

Signature _____

Date _____

APPOINTMENT AFFIDAVITS

(Position to which Appointed)

(Date Appointed)

VA CONNECTICUT _____

WEST HAVEN/NEWINGTON _____

(Department or Agency)

(Bureau or Division)

(Place of Employment)

I, do solemnly swear (or affirm) that--

A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

(Signature of Appointee)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

EMERGENCY CONTACTS

Resident/Fellow Name: _____

Current Address: _____

Local Telephone: _____

Anticipated CT Address (if known and different from above):

Name/phone of person to be contacted in case of emergency:

Name: _____ Daytime Phone: _____

Name/phone of Secondary emergency contact person:

Name: _____ Daytime Phone: _____

APPLICATION FOR USER ACCOUNT

VA Connecticut Healthcare System

950 Campbell Avenue
West Haven, Connecticut 06516
Information Resources Management Service (IRM)

USER IDENTIFICATION (Please print "clearly"):

LAST NAME	FIRST NAME	M.I.
SOCIAL SECURITY NUMBER		
111		

ROUTING SYMBOL	USER'S SIGNATURE
.....	

ACCESS REQUESTED*:

INTERN/FELLOW
POSITION TITLE OF USER

ATV Healthcare Provider Menu
PRIMARY MENU OPTIONS

ORES, MAGDISP CLIN

SECURITY KEYS

SECONDARY MENU OPTIONS

Student
TIU USER CLASS

ORZ-ADD-ORD-CLINICIAN-MED
CPRS ADD ORDER SCREEN

ADPAC SIGNATURE

***To be completed by ADPAC or Service Chief only.**

ACCESS AUTHORIZATION (IRM):

DATE COMPLETED

IRM PERSONNEL SIGNATURE

September 18, 2007 VA Handbook 6500 Appendix G G-3

Department of Veterans Affairs (VA) National Rules of Behavior

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 when I use any Government information system, I have NO expectation of Privacy in VA records that I create or in my activities while accessing or using such information system.

b. 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 Information Security Officers (ISOs). Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized Office of Inspector General (OIG), VA, and law enforcement personnel.

c. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting 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.

d. I understand that such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal, civil, and/or administrative 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.

e. I understand that I have a responsibility to report suspected or identified information security incidents (security and privacy) to my Operating Unit's Information Security Officer (ISO), Privacy Officer (PO), and my supervisor as appropriate.

f. 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 supervisor, 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.

g. I understand that the VA National Rules of Behavior 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 United States Government.

h. I understand that the VA National Rules of Behavior do not supersede any local policies that provide higher levels of protection to VA's information or information systems. The VA National Rules of Behavior provide the minimal rules with which individual users must comply.

i. I understand that if I refuse to sign this VA National Rules of Behavior as required by VA policy, I will be denied access to VA information and information systems. Any refusal to sign the VA National Rules of Behavior may have an adverse impact on my employment with the Department.

2. SPECIFIC RULES OF BEHAVIOR.

a. I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor and the ISO when the access is no longer needed.

- b. I will follow established VA information security and privacy policies and procedures.
- c. I will use only devices, systems, software, and data which I am authorized to use, including complying with any software licensing or copyright restrictions. This includes downloads of software offered as free trials, shareware or public domain.
- d. I will only use my access for authorized and official duties, and to only access data that is needed in the fulfillment of my duties except as provided for in VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. I also agree that I will not engage in any activities prohibited as stated in section 2c of VA Directive 6001.
- e. I will secure VA sensitive information **in all areas** (at work and remotely) and in any form (e.g. digital, paper etc.), to include mobile media and devices that contain sensitive information, and I will follow the mandate that all VA sensitive information must be in a protected environment at all times or it must be encrypted (using FIPS 140-2 approved encryption). If clarification is needed whether or not an environment is adequately protected, I will follow the guidance of the local Chief Information Officer (CIO).
- f. I will properly dispose of VA sensitive information, either in hardcopy, softcopy or electronic format, in accordance with VA policy and procedures.
- g. 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.
- h. I will not attempt to alter the security configuration of government equipment unless authorized. This includes operational, technical, or management security controls.
- i. I will protect my verify codes and passwords from unauthorized use and disclosure and ensure I utilize only passwords that meet the VA minimum requirements for the systems that I am authorized to use and are contained in Appendix F of VA Handbook 6500.
- j. I will not store any passwords/verify codes in any type of script file or cache on VA systems.
- k. I will ensure that I log off or lock any computer or console before walking away and will not allow another user to access that computer or console while I am logged on to it.
- l. I will not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any VA electronic communication system.
- m. I will not auto-forward e-mail messages to addresses outside the VA network.
- n. I will comply with any directions from my supervisors, VA system administrators and information security officers concerning my access to, and use of, VA information and information systems or matters covered by these Rules.
- o. I will ensure that any devices that I use to transmit, access, and store VA sensitive information outside of a VA protected environment will use FIPS 140-2 approved encryption (the translation of data into a form that is unintelligible without a deciphering mechanism). This includes laptops, thumb drives, and other removable storage devices and storage media (CDs, DVDs, etc.).
- p. I will obtain the approval of appropriate management officials before releasing VA information for public dissemination.,
- q. I will not host, set up, administer, or operate any type of Internet server on any VA network or attempt to connect any personal equipment to a VA network unless explicitly authorized **in writing** by my local CIO and I will ensure that all such activity is in compliance with Federal and VA policies.
- r. I will not attempt to probe computer systems to exploit system controls or access VA sensitive data for any reason other than in the performance of official duties. Authorized penetration testing must be approved in writing by the VA CIO.
- s. 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.

t. I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by the VA on VA equipment or on computer systems that are connected to any VA network.

u. If authorized, by waiver, to use my own personal equipment, I must use VA approved virus protection software, anti-spyware, and firewall/intrusion detection software and ensure the software is configured to meet VA configuration requirements. My local CIO will confirm that the system meets VA configuration requirements prior to connection to VA's network.

v. I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee at the time of system problems.

w. I will not disable or degrade software programs used by the 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.

x. I agree to allow examination by authorized OI&T personnel of any personal IT device [Other Equipment (OE)] that I have been granted permission to use, whether remotely or in any setting to access VA information or information systems or to create, store or use VA information.

y. I agree to have all equipment scanned by the appropriate facility IT Operations Service prior to connecting to the VA network if the equipment has not been connected to the VA network for a period of more than three weeks.

z. I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional required training for the particular systems to which I require access.

aa. I understand that if I must sign a non-VA entity's Rules of Behavior to obtain access to information or information systems controlled by that non-VA entity, I still must comply with my responsibilities under the VA National Rules of Behavior when accessing or using VA information or information systems. However, those Rules of Behavior apply to my access to or use of the non-VA entity's information and information systems as a VA user.

bb. 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.

cc. 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 must use VA-provided IT equipment for remote access when possible. I may be permitted to use non-VA IT equipment [Other Equipment (OE)] only if a VA-CIO-approved waiver has been issued and the equipment is configured to follow all VA security policies and requirements. I agree that VA OI&T officials may examine such devices, including an OE device operating under an approved waiver, at any time for proper configuration and unauthorized storage of VA sensitive information.

dd. I agree that I will not have both a VA network connection and any kind of 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 local CIO.

ee. I agree that I will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and approved in advance by the appropriate VA official (supervisor), and a waiver has been issued by the VA's CIO. I agree that I will not access, transmit or store remotely any VA sensitive information that is not encrypted using VA approved encryption.

ff. I will obtain my VA supervisor's authorization, in writing, prior to transporting, transmitting, accessing, and using VA sensitive information outside of VA's protected environment..

gg. 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 that authorized OI&T personnel may periodically inspect the remote location for compliance with required security requirements.

hh. I will protect sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by the VA to protect sensitive data.

ii. I will not store or transport any VA sensitive information on any portable storage media or device unless it is encrypted using VA approved encryption.

jj. I will use VA-provided 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. VA sensitive information includes personally identifiable information and protected health information.

kk. I may be required to acknowledge or sign additional specific or unique rules of behavior in order to access or use specific VA systems. I understand that those specific rules of behavior 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.

a. I acknowledge that I have received a copy of these Rules of Behavior.

b. I understand, accept and agree to comply with all terms and conditions of these Rules of Behavior.

Signature

Date

Office Phone Position Title

FINGERPRINTING INFORMATION

Every individual with a qualified need to have access to the VA Connecticut Healthcare System (VACT) computer system will now have to be fingerprinted. As a Fellow/Resident/Student/Trainee, you will require such access; therefore, you will need to get this done. Failure to get this done prior to your scheduled start date will result in the delay of your training at the VACT.

If you would like to get this done at a VA facility that is closer to you, please contact the responsible people below to make arrangements.

If you get this done prior to orientations you can get a badge before your start date. In the very near future you will be **required** to use your VA ID badge to log onto the computer. If you have a PIV badge from another hospital, please let Liz Castellon know about this.

We understand that prior to your start date at the VACT you may have significant constraints on your time; however, please try and get this completed.

If you have any questions regarding this requirement, please contact at Liz Castellon or Derek Waxman at 203-932-5711 ext 2704 or Elizabeth.Castellon@va.gov or Derek.Waxman@va.gov

For names beginning with A - L

Sandra LK Masciullo

Personnel Security Specialists, HRMS/05B, Bldg 4, Rm D-103A

Sandy Hrs: Monday-Friday, 7:30-3:30

Email: sandra.masciullo@va.gov

Phone: 203-932-5711 x2417

For names beginning with M - Z

Carol Mollison

Personnel Security Specialists, HRMS/05B, Bldg 4, Rm D-103A

Carol Hrs: Monday-Friday 8:30-4:00

Email: carol.mollison@va.gov

Phone: 203-932-5711 x7934

YOU MUST CHECK ONE AND PROVIDE ALL REQUESTED INFORMATION:

REGULAR EMPLOYEE FEE BASIS VOLUNTEER WOC PHYSICIAN ATTENDING
RESEARCH DEPT (WOC)
STUDENT _____ (INCLUDE SCHOOL NAME) LENGTH OF APPT _____
RESIDENT / INTERN / FELLOW SERVICE NAME _____ LENGTH OF APPT _____
CONTRACT EMPLOYEE _____ VENDOR COMPANY NAME _____

STATION WH Newington Rocky Hill VH&Hospital UCONN

The following information is required in order to submit your fingerprints which will be taken by Human Resources as a part of processing your appointment or in connection with the reinvestigation required due to the risk level associated with your position.

DATE: _____ **EMAIL ADDRESS:** _____

DEPARTMENT WORKING/ROTATING IN: _____ Medicine _____

PERSONAL:

POSITION TITLE: _____ Resident/Fellow Medicine _____ (Resident enter Resident-and the practice. For example: Resident-Medicine, Resident-Psychology, etc...) (If contractor, you must enter Contractor and then either the contract number or vendor name):

NAME (Full Name): _____
LAST FIRST FULL MIDDLE NAME AT BIRTH

ALIASES: _____ **PHONE NUMBER** _____
MAIDEN NAME, DIVORCED NAMES, ETC.

SSN (full): _____ **DOB:** _____

ADDRESS: _____
COMPLETE STREET ADDRESS (Include Apt #, Suite #, etc.), CITY STATE ZIP

COUNTRY OF CITIZENSHIP: _____ **US CITIZEN:** [] YES [] NO IF NO – COUNTRY _____

PLACE OF BIRTH: _____

USA:
CITY _____ STATE _____

OUTSIDE USA: _____
CITY/TOWN/VILLAGE/TERRITORY/PROVINCE COUNTRY

PHYSICAL:

GENDER: _____ MALE / FEMALE _____

RACE: _____ A-ASIAN, B-BLACK, I-NATIVE AMERICAN, W-CAUCASIAN/LATINO, U-UNKNOWN

EYES: _____ BLK-BLACK, BLU-BLUE, BRO-BROWN, GRN-GREEN, GRY-GRAY, HAZ-HAZEL, PNK-PINK, MAR-MAROON, MUL-MULTICOLORED, XXX-UNKNOWN

HAIR: _____ BAL-BALD, BLK-BLACK, BLN-BLONDE/STRAWBERRY, BLU-BLUE, BRO-BROWN, GRN-GREEN, GRY-GRAY/PARTIALLY, ONG-ORANGE, PLE-PURPLE, PNK-PINK, RED-RED/AUBURN, SDY-SANDY, WHI-WHITE, XXX-UN KNOWN

HEIGHT: _____ (FEET/INCHES) **WEIGHT:** _____ (POUNDS)

VACT FINGERPRINTER _____ **DATE** _____ **EQUIP** [] YES [] NO **REVISED**
11/27/2012

YOU MUST COMPLETE THIS TRAINING AND RETURN THE CERTIFICATES WITH YOUR PAPERWORK OR YOU WILL NOT GET COMPUTER ACCESS.

IF YOU ALREADY HAVE AN ACCOUNT AT THE VA THAT YOU ARE PRESENTLY AT PLEASE FORWARD A COPY OF YOUR CURRENT CERTIFICATE.

Dear VA Health Professions Trainee,

You may be selected, through an affiliation agreement between Yale School of Medicine and Department of Veterans Affairs to receive an appointment in a health professions training program at the VA Connecticut Healthcare System, Medical Service.

VHA Mandatory Training for Trainees

In order for you to train at VA, you are required to complete a mandatory training program titled *VHA Mandatory Training for Trainees*. This training is available through the VA Talent Management System (TMS). The TMS offers web-based training to VA employees and its partners.

To use the TMS, you must self-enroll and create a profile at <http://www.tms.va.gov>. Once you are at the TMS website, follow the steps listed below to create your profile, launch the mandatory training course and complete the content prior to your coming to VA to begin your clinical training. Items noted in red should be entered on your profile.

Managed Self-Enrollment (MSE) enhances VA's training and reporting compliance, and is another step toward establishing VA as a 21st century organization built on providing the best care and service possible for our Veterans!

If you have any questions or require additional information, please do not hesitate to contact me at (203) 932-5711 Ext. 2704. If you need to leave a message, please be sure to leave a contact number and best time to call. You can also email me with any questions or concerns.

Sincerely,

Liz

Liz Castellon
West Haven Medical Center
Medical Services
Phone: 203-932-5711, Ext. 2704
Fax: 203-937-3425
Email: elizabeth.castellon@va.gov

Step-by-Step Instructions

1. From a computer, launch a web browser and navigate to <http://www.tms.va.gov>
2. Click the [**Create New User**] link located near the SIGN IN button.
3. Select the radio button for “**Health Professions Trainee**” *DO NOT SELECT "WOC"*
4. Click the [**Next**] button
5. Complete all required fields, and any non-required fields if possible.
 - a. **My Account Information:**
 - i. Create Password
 - ii. Re-enter Password
 - iii. Security Question
 - iv. Security Answer
 - v. Social Security Number* *(If you do not have a Social Security Number, follow the on-screen instructions when registering.)*
 - vi. Re-enter Social Security Number
 - vii. Date of Birth
 - viii. Legal First Name
 - ix. Legal Last Name
 - x. eMail Address *(Enter your personal email address. The eMail address will be used as your UserID when you login)*
 - xi. Re-enter eMail address
 - xii. Phone Number *(Enter a number where you can be reached by VA staff if issues arise with this self-enrollment process or in other circumstances)*

b. My Job Information:

- i. VA City – **(West Haven)**
- ii. VA State – **(CT or Connecticut)**
- iii. VA Location Code – **(CON(VA Connecticut Healthcare System))**
- iv. Trainee Type – **(Physician Residents)**
- v. Specialty/Discipline – **(Medicine)**
- vi. VA Point of Contact First Name - **(Elizabeth)**
- vii. VA Point of Contact Last Name - **(Castellon)**
- viii. VA Point of Contact Email **(elizabeth.castellon@va.gov)**

Once you have entered all of the required data, click the “**Submit**” button. Your profile will be immediately created. Copy and save the **UserID** displayed to you on the confirmation page, as you will need this for future logons to the VA TMS. Once done, click on the “**Continue**” button and wait until your “**To-Do**” list is displayed with the title of the mandatory training course.

Launching and Completing the Content

1. Mouse over the title of the *VHA Mandatory Training for Trainees* training course.
2. Click the [**Go to Content**] button in the pop-up window that appears.
3. Complete the course content following the on-screen instructions.
4. Exit the course and a completion of the course will be recorded for your effort.
5. Click on the “**Completed Work**” pod on the lower right hand side of your internet browser window.

6. Move your mouse over the title of the course you just completed and choose to “**Print Completion Certificate**”.
7. Print your completion certificate and save it in a pdf file for your records.
8. You can either email or fax your **Certificate of Completion** to Liz Castellon at Elizabeth.castellon@va.gov or fax to (203) 937-3425.

Trouble-shooting and Assistance

The **Check System** link on the VA TMS is an automated tool that confirms the existence of basic, required software on the computer you are using to complete this training. If one of the components of your computer is not in compliance with the requirements, a red “x” will appear next to the **Check System** link. Should this be the case with your computer, please follow the instructions to bring your computer up to the standards that will work with the VA TMS.

If you do not have a Social Security Number, or if you experience any difficulty creating a profile or completing the mandatory content, contact the VA MSE Help Desk at 1.888.501.4917 or via email at VAMSEHelp@gpworldwide.com.

* Your SSN is used only as a unique identifier in the system to ensure users do not create multiple profiles. The SSN is stored in a Private Data Table that cannot be accessed anywhere via the VA TMS interface. It is securely transferred to a VA database table inside the VA firewall where it can be confirmed, if necessary, by appropriately vested system administrators and/or Help Desk staff.