

MY HEALTH_eVET IN-PERSON AUTHENTICATION

- 1. REASON FOR ISSUE.** This Veterans Health Administration (VHA) Handbook establishes guidance on procedures for Release of Information (ROI) staff to perform an In-person Authentication (IPA) for every veteran requesting initial access to Individually-identifiable Health Information within My Health_eVet (MHV).
- 2. SUMMARY OF CHANGES.** This VHA Handbook provides new guidance on how veterans who have a Legal Guardian or a Power of Attorney can meet the requirements for IPA.
- 3. RELATED ISSUES.** VHA Directive 1605.
- 4. FOLLOW-UP RESPONSIBILITY.** The Office of Information (19) is responsible for the contents of this Handbook. Questions may be referred to the Director of Health Data and Informatics at 202-461-5874.
- 5. RECISSIONS.** VHA Handbook 1907.02, dated January 8, 2007, is rescinded.
- 6. RECERTIFICATION.** This VHA Handbook is scheduled for recertification on or before the last working day of June 2013.

Michael J. Kussman, MD, MS, MACP
Under Secretary for Health

DISTRIBUTION CO: E-mailed 6/27/08
FLD: VISN, MA, DO, OC, OCRO, and 200 – E-mailed 6/2708

CONTENTS

MY HEALTH_eVET IN-PERSON AUTHENTICATION

PARAGRAPH	PAGE
1. Purpose	1
2. Background	1
3. Scope	1
4. Definitions	1
5. Responsibilities	2
6. In-person Authentication Process	2
7. In-person Authentication for Veterans who have a Legal Guardian or a General Power of Attorney	5
8. Unable to Authenticate Process	5

MY HEALTH_eVET IN-PERSON AUTHENTICATION

1. PURPOSE

This Veterans Health Administration (VHA) Handbook establishes procedure for Release of Information (ROI) staff to perform an In-person Authentication (IPA) for every veteran requesting initial access to Individually-identifiable Health Information within My Health_eVet (MHV).

2. BACKGROUND

a. The Privacy Act, Title 5 United States Code (U.S.C.) 552a, implemented by Title 38 Code of Federal Regulations (CFR) §575-1.584, provides for the confidentiality of Individually-identified and retrievable information about living individuals which is maintained in a Privacy Act system of records.

b. The Health Insurance Portability and Accountability Act (HIPAA), Public Law (Pub. L.) 104-191, implemented by 45 CFR Parts 160 and 164, establishes standards and requirements for the electronic transmission, privacy, and security of certain health information.

3. SCOPE

VHA must perform an IPA to verify the identity of the veteran when initial access is requested by that veteran for MHV's enhanced benefits (e.g., copies of key portions of the VHA electronic health record).

4. DEFINITIONS

a. **Enhanced Benefits.** For the purpose of this Handbook, enhanced benefits applies to access to electronic copies of an individual's health information, such as a discharge summary or problem list.

b. **Individually-identifiable Health Information.** For the purpose of this Handbook, Individually-identifiable Health Information is any information, including health information maintained by VHA, pertaining to an individual that also identifies the individual.

c. **In-person Authentication (IPA).** IPA is the act of verifying a veteran's identity.

d. **My Health_eVet (MHV).** MHV is a web-based application that provides veterans access to a secure, private, electronic copy of their own VHA health information.

e. **MHV Registration.** MHV registration is the processing of a user's request for an MHV account and creation of a username and password, after they have read and accepted MHV's terms and conditions.

f. **Overprinted VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information.** For the purpose of this Handbook, overprinted VA Form 10-5345a is the form signed by the veteran to indicate all prerequisites have been met; this satisfies the criterion for a written request for copies of the veteran's records.

g. **Release of Information (ROI).** ROI is the act of providing copies of Individually-identifiable Health Information.

h. **Sensitive Information.** For the purposes of this Handbook sensitive information is health information that, with a reasonable degree of medical certainty, is likely to have a serious adverse effect on an individual's mental or physical health if it is revealed to the individual.

5. RESPONSIBILITIES

a. **Facility Director.** The facility Director is responsible for ensuring that ROI staff, or other assigned staff, understand their role and receive appropriate access and instructions on the use of the MHV administrative portal and the IPA process (see par. 6).

b. **Health Information Manager or Privacy Officer.** The Health Information Manager, or Privacy Officer, is responsible for training the ROI staff or other assigned staff to perform the IPA.

c. **MHV Project Team.** The MHV project team is responsible for providing and maintaining functionality that facilitates the IPA.

d. **Health Care Facility ROI Staff, or Other Assigned Staff.** The ROI staff, or other assigned staff, is responsible for the IPA of every veteran requesting initial access to Individually-identifiable Health Information through MHV.

6. IN-PERSON AUTHENTICATION PROCESS

In order to ensure that access to a veteran's individual health information is granted only to the individual to whom the information pertains, every veteran requesting initial access must be verified or authenticated.

a. The ROI staff, or other assigned staff, must ensure, through the IPA process, that the appropriate veteran is given access to the right information. IPA can be performed in the medical center, in a Community-based Outpatient Clinic (CBOC), or other location that is staffed with VA employees trained to perform authentication and who have access to the MHV administration portal. The authentication process is only required initially, and once authenticated, the veteran has access to all information released by MHV, regardless of location.

b. In order to be authenticated the veteran must:

- (1) Be a MHV registered user,
- (2) Be matched to the Master Patient Index (MPI),

- (3) Be verified within MHV as a patient at a VA medical center,
- (4) View the MHV orientation video,
- (5) Complete and sign the overprinted VA Form 10-5345a, and
- (6) Present one form of government-issued photo identification.

c. When there is a request by a veteran for access to electronic copies of individually-identifiable health information using MHV, the ROI staff, or other assigned staff, must first perform an IPA. An IPA is required prior to granting access to health information. IPA is only required on initial access and once authenticated a veteran is able to access all available information from any facility at which the veteran has been seen. The IPA process may be performed at any facility, regardless of whether the Veteran is a patient at that facility; however the veteran must be a patient in a VA facility.

NOTE: A limited number of Veterans Integrated Service Network (VISN) 22 veterans, who are currently enrolled in a system with features similar to MHV, will have the option of using an alternative approach for MHV IPA. This approach is time-limited to 3 months after the availability of Individually-identifiable Health Information. After the 3 month period, all veterans not previously enrolled in the VISN 22 system, will be required to enroll in MHV and be authenticated.

d. When a veteran requests initial access to Individually-identifiable Health Information through MHV, ROI or other assigned staff must:

- (1) Require the veteran to present one form of government-issued photo identification,
- (2) Log in to the administration portal within MHV using a unique User Identification (ID) and password, and
- (3) Select the tab for IPA.

e. When the MHV User screen is presented to ROI staff, or other assigned staff, they can search for a MHV user either by first letter of last name and last four digits of the Social Security Number (SSN), User ID, or by personal data provided by the veteran (first name, last name, SSN, date of birth (DOB)). Search results are returned in the default order following:

- (1) Last name in alphabetical order,
- (2) First name in alphabetical order, and
- (3) MHV User ID in ascending order

f. ROI staff, or other assigned staff, may further sort search results based on any of the information displayed.

(1) If there are no MHV users that match the search criteria, then the following message is displayed: “No MHV Users were found for the search criteria entered. Please verify that the person is a registered MHV user and try another option below.”

(a) If the veteran has not previously registered for MHV, and been matched to the MPI, and verified as a VA medical center user, the ROI or other assigned staff will not be able to locate the veteran within the user screen and thus be unable to authenticate the veteran.

(b) If the veteran wishes to become a MHV registered user or needs assistance with any of the other requirements, the veteran is to be referred to the individual at the medical center who is the MHV point of contact (POC) for assistance.

(2) If the authentication process cannot be completed due to missing prerequisites or there is a need to perform a review of the record for information that may be sensitive to the veteran, the authentication process may be deferred or placed on hold.

g. The ROI staff, or other assigned staff, must select a reason for deferring authentication.

h. The system displays a message confirming the selections have been saved. The Authentication Status for the MHV user is updated to indicate authentication is in-process.

i. If there is a match within MHV, the screen displays the matching record(s) corresponding to the search criteria entered in the Search MHV User screen. If the record returned matches the veteran requesting authentication and an IPA has not been previously completed, the assigned staff selects the record to initiate or complete the authentication process for that MHV user.

j. The veteran presents the assigned staff with the completed overprinted VA Form 10-5345a.

k. The ROI staff, or other assigned staff, reviews the form for completeness, checks the appropriate boxes within the MHV system, and completes the authentication process. If the veteran has not completed all of the prerequisites, the ROI staff, or other assigned staff saves the screen selection in order to complete authentication at a later date. **NOTE:** *The completed VA Form 10-5345a needs to be scanned using Veterans Health Information Systems Technology Architecture (VistA) Imaging Indexing or Administration, or Document or Image, Type: ROI. Change the image description to MHV, lock it in, and make a scan tab called MHV. The date of document is the date the overprinted VA Form 10-5345a was signed.*

l. The assigned staff must verify, by reviewing the Confirm User Authentication Screen, that the IPA process has been completed.

m. Once IPA has been completed, the ROI staff must perform a record review of all information that is to be released by MHV to determine if any information that is potentially sensitive to the veteran exists. **NOTE:** *Refer to the MHV Handbook for Record Review for complete process and procedure.*

7. IN-PERSON AUTHENTICATION FOR VETERANS WHO HAVE A LEGAL GUARDIAN OR A GENERAL POWER OF ATTORNEY

a. Veterans who are unable to act on their own behalf either have a Legal Guardian (LG) or have provided someone with a general power of attorney (POA) (provided such General Power of Attorney specifically states the POA has the authority to request copies of health records on the veteran's behalf), can still receive the enhanced benefits of My Health_eVet.

b. In order to receive the benefits of IPA, the LG or POA must:

(1) Go to the medical center or CBOC and request IPA.

(2) Complete all of the prerequisites required as outlined in this Handbook, and:

(a) Present a government-issued photo identification for both themselves and the veteran for whom they are requesting an IPA;

(b) Sign VA Form 10-5345a, on behalf of the veteran, to demonstrate that all prerequisites have been completed by the LG or POA;

(c) Present a written, signed (by the veteran), dated, and notarized copy of the POA that specifically names the individual who is acting on behalf of the veteran and specially grants the right to request health records on the veteran's behalf; or

(d) Present the court appointment that specifically grants guardianship to the individual who is requesting authentication in the veteran's stead.

c. All documents and requests for authentication by either a LG or a POA must be carefully reviewed by the Chief, Health Information Management, the Privacy Officer, or the ROI supervisor to ensure that the person requesting authentication has the authority to do so on behalf of the veteran. Copies of the POA or legal guardianship must be scanned and retained along with the signed VA Form 10-5345a.

8. UNABLE TO AUTHENTICATE PROCESS

If a member of the ROI staff, or assigned staff, is the veteran, be aware that a staff member cannot authenticate oneself. If the MHV user selected from the list of users has the same first name and last name as the assigned staff, then the MHV user cannot be authenticated and the following message is displayed: "Cannot Authenticate. You cannot authenticate yourself. A different assigned staff must authenticate you."

a. **Termination of Authentication Process.** Once the authentication process has started and the authenticating facility has been selected, any of the prerequisites have been checked as completed, reason for delay has been selected, or approved for authentication has been checked, none of the preceding can be deselected. If an error has been made in any of those areas, the authentication process must be terminated and started again.

b. **Removal of Authentication.** Occasionally it may be necessary to remove the authentication of a veteran who has been previously authenticated. This option is only used in the rare circumstances when access to one veteran's records has been given to the incorrect veteran. The process is as follows:

- (1) The ROI staff, or other assigned staff, chooses an authenticated MHV User from which to remove authentication.
- (2) The system displays the date when the MHV User was authenticated.
- (3) The ROI staff, or other assigned staff, specifies a reason for removing authentication and selects the appropriate reason to remove authentication for the MHV User.
- (4) The system asks the authenticator to confirm removing authentication for the MHV User.
- (5) The ROI staff, or other assigned staff, confirms removing authentication.
- (6) The system displays a confirmation message indicating authentication has been removed for the MHV User. The Authentication Status for the MHV User is updated to indicate the MHV User is no longer authenticated.