

September 23, 2003

DISASTER EMERGENCY MEDICAL PERSONNEL SYSTEM (DEMPS) PROGRAM AND DATABASE

1. PURPOSE: This Veterans Health Administration (VHA) Directive provides policy regarding the Disaster Emergency Medical Personnel System (DEMPS) Program and database.

2. BACKGROUND

a. The DEMPS Program, described in the Veterans Health Administration (VHA) Handbook 0320.3, was developed to identify and collect information on VHA personnel who may be available to be deployed in an emergency.

b. The DEMPS database is maintained on the Emergency Management Strategic Healthcare Group (EMSHG) web site (<http://vaww.va.gov/emshg/>). The database is accessible via the VA Intranet only. The database is covered under DEMPS-VA (98va104A) System of Records Notice. Access to the DEMPS database requires the use of Public Key Infrastructure (PKI) for encryption and access.

3. POLICY: It is VHA policy that a DEMPS be established for use during times of national disasters and VA emergencies; that information on VHA personnel who register as volunteers be maintained in the DEMPS database; and that no facility staff may be deployed without the VA Medical Center Director's approval.

4. ACTION

a. **Veterans Integrated Service Network (VISN) Director.** The VISN Director is responsible for:

(1) Ensuring DEMPS volunteer recruitment processes are in place.

(2) Receiving quarterly reports on the number of VISN DEMPS volunteers from respective EMSHG VISN-Liaison Area Emergency Managers (AEMs).

b. **VA Medical Center Director.** The VA Medical Center Director is responsible for:

(1) The implementation and maintenance of the DEMPS Program for the medical center through a recruitment program that ensures staff members are informed about DEMPS.

(2) Designating a primary and secondary DEMPS coordinator who are responsible for recruitment, providing information to staff on the DEMPS, and maintaining local information in the DEMPS database for the VA medical center.

THIS VHA DIRECTIVE EXPIRES SEPTEMBER 30, 2008

VHA DIRECTIVE 2003-052

September 23, 2003

(3) Ensuring that primary and secondary DEMPS coordinators obtain passwords for DEMPS database access.

(4) Providing the EMSHG VISN Liaison AEM with the names, e-mail addresses, and phone numbers of the assigned coordinators.

c. **Primary and Secondary Coordinator.** The Primary and Secondary Coordinator are responsible for:

(1) Obtaining the Public Key Infrastructure (PKI) password and for entering and maintaining volunteer information in the VA medical center's DEMPS database.

(2) Coordinating facility DEMPS volunteer recruitment activity.

(3) Contacting volunteers, at least annually, to ensure they wish to remain volunteers and to update information. *NOTE: Application instructions are in Attachment A.*

d. **EMSHG.** EMSHG is responsible for:

(1) Maintaining a consolidated list of all Primary and Secondary DEMPS Coordinators.

(2) Providing the DEMPS report to VHA Central Office.

(3) Maintaining the web site containing the DEMPS database.

(4) Supporting the DEMPS efforts of AEMs.

(5) Providing periodic reports on the number and categories of DEMPS volunteers to the Under Secretary for Health.

e. **AEM.** AEMs are responsible for:

(1) Supporting the VISN DEMPS Program by assisting the facility coordinators in recruitment, by providing educational briefings and/or information, and by assisting with PKI applications.

(2) Assisting Directors and the DEMPS Coordinators with implementing and maintaining the DEMPS Program.

5. REFERENCES: VHA Handbook 0320.3

6. FOLLOW-UP RESPONSIBILITY: EMSHG (13C) is responsible for the contents of this Directive. Questions may be addressed to 304-264-4835.

7. RESCISSION: VHA Directive 2002-014, dated March 7, 2002, is rescinded. This VHA Directive expires September 30, 2008

S/ Nevin M. Weaver for
Robert H. Roswell, M.D.
Under Secretary for Health

Attachment

DISTRIBUTION: CO: E-mailed 9/23/03
FLD: VISN, MA, DO, OC, OCRO, and 200 – E-mailed 9/23/03

ATTACHMENT A

APPLICATION PROCEDURES FOR DEMPS ACCESS

1. Each Department of Veterans Affairs (VA) medical facility Director identifies both a Primary and a Secondary Disaster Emergency Medical Personnel System (DEMPS) Coordinator who are responsible for entering, editing, and deleting records in the DEMPS database. **NOTE:** *Facility Directors may wish to consider providing "read only" access to a limited number of other facility personnel who may assist with personnel management; these personnel also require access to the database.*
2. Once the Director approves the Primary and Secondary DEMPS Coordinators, names of these individuals, their locations with complete mailing addresses, e-mail addresses, phone numbers, and required access (either "enter/edit" or "read only") must be provided to the respective Emergency Management Strategic Healthcare Group (EMSHG) Veterans Integrated Service Network (VISN) Liaison Area Emergency Manager (AEM).
3. Once reviewed and verified by the EMSHG VISN Liaison AEM, the information is forwarded to the facility Information Security Officer (ISO) for processing. The AEM must contact the EMSHG Program Manager, Information Resources, to request access for each coordinator and provide the name of the facility for which they will need access. **NOTE:** *Questions may be referred to the DEMPS Program Manager (contact information found on the EMSHG web site <http://vaww.va.gov/emshg>).*
4. After receipt of the application, a Public Key Infrastructure (PKI) packet, including a Personal Identification Number (PIN) will be given directly to the individual. To receive the PIN, individuals may be required by the ISO to provide proof of identification through a picture identification (ID).
5. When the PIN is issued, the individual must go to: <https://vaww.va.gov/vapki2> to complete the application enrollment and obtain the verification certificate.
6. PKIs must be renewed annually.
7. Coordinators and EMSHG VISN Liaison AEMs must work together in the development of a robust recruitment program.


[VA PKI Home](#)
[For PKI Users](#)
[Project Management](#)
[Documents](#)
[Links](#)
[Participants](#)

Department of Veterans Affairs

Internal Staff

Digital ID Center

[Help](#)

**Before proceeding with your enrollment, please download and read the following

[USER GUIDE](#)

**

Also, please visit the

["Getting Started"](#)

section of the "For PKI Users" page to get answers to all of your PKI related questions.

****Please make sure to make a backup of your PKI keys on a floppy disk.**

If you have questions about the options listed on this page, please read our [F.A.Q. Document](#) or contact the VA PKI Help Desk via e-mail at vapkihelp@med.va.gov or by phone at (703)848-2898.

More detailed documentation is available by visiting the ["For PKI Users"](#) page or by clicking on the "For PKI Users" button on the left side of this page.



ENROLL...

• [for Encryption and Signing Digital ID](#)

***** Because of important security patches recently released by Microsoft in September of 2002, it is imperative that you contact the person with administrative rights to your p.c. to upgrade your browser before proceeding further, otherwise you may receive a "1B6" error during your registration. For more information on this, please refer to Microsoft Security Bulletin Q323172 or the Microsoft Knowledge Base article MS02-048.*****



SEARCH

Choose this option to find the record for a Digital ID. This function is useful for determining whether a Digital ID is Valid, Expired, or Revoked. You may also Download IDs from this option.



RENEW

Choose this option to renew a Digital ID which is expiring or which has already expired. You should generally start renewing your Digital ID at least one month before your Digital ID is due to expire or when you receive a renewal notice by e-mail from the system administrator. **You must click on each link separately below to receive your complete dual key pair.**

• [for Encryption Digital ID](#)

• [for Signing Digital ID only](#)



REVOKE

Choose this option to revoke your Digital ID. Digital IDs should be revoked immediately for any suspected compromise, including lost or stolen private keys, corrupted key pairs, change in site ownership, or suspected fraud.

If you would like to learn more about Digital ID's and how they work, please read [Verisign's F.A.Q.](#)