Testimony of Gail Graham
Veterans Health Administration
AHIC Workgroup
September 29, 2006

Good afternoon. I am Gail Graham, Director of Health Data & Informatics for the Department of Veterans Affairs, Veterans Health Administration. Thank you for the opportunity to share our experience with identity proofing and user authentication in our personal health record program.

On Veterans Day in 2003, the Department of Veterans Affairs launched My Health***e***Vet, a gateway to veteran health benefits and services. A year later, VA added the Personal Health Journal, a convenient and secure on-line journal veterans can use to manage their health information. My Health***e***Vet was designed to provide health information developed especially for veterans. In addition to the Personal Health Journal, the site provides access to a health information library, links to Federal and VA benefits and resources, health calculators and self-assessment tools, and online VA prescription refill. In the future, users will be able to view appointments, copay balances, and key portions of their VA health records online.

Identity proofing and user authentication is handled in the My Health***e***Vet Personal Health Record in a tiered model that aligns increasingly rigorous requirements with an increasing level of access to information.

- Website visitors may access patient health education content through the site's evidence-based health information libraries without registering or logging in.
- Registration is required before users can access additional program features. Initial registration is accomplished using a web-based form on the site, and complex passwords

are required in order to safeguard user information. Once registered, users have access to self-entered information features such as health journals and health e-logs.

- In order to enable the inclusion of personally-identifiable health information from the electronic medical record, "heavy proofing" is required through in-person authentication (IPA). To accomplish this level of authentication, veterans must present at a VA Facility or VA-designated location and display a photo ID or a new Veterans Identification Card (VIC). Valid photo ID may include a driver's license, passport, or other government ID. My Health***e***Vet Registration then initiates a transactional process to match the user's information with the VA Master Patient Index (MPI), using the Social Security Number as a key identifier. This matching is critical to connect the patient to functions like prescription refill (which is available now) and health information extracts (which will be available later this year).

For example, a patient seeking access to parts of his or her electronic health record through My Health***e***Vet would go to a VA Medical Center to be identified face-to-face by the facility's Release of Information (ROI) office. The ROI staff would ask the patient for appropriate identification and verify the patient's information in VistA, VHA's electronic health record. This authentication process would only be required to be completed once. Once the patient was identified and authenticated, the patient would receive access to request copies of his or her electronic health record through My Health***e***Vet.

My Health***e***Vet currently contains data entered by the health care consumer, and may soon include a copy of key portions of the patient's electronic medical record, extracted and integrated securely into the patient's PHR. In a future release, patients will be able to delegate access to

one part or all parts of the PHR to another person (such as a health care provider, family member, and advocate).

This functionality has been tested as part of the My HealtheVet Pilot at 9 VA Medical Centers; the pilot has supported more than 7,000 users over the past several years with positive results. The pilot enables participants to request extracts from their VA EHR, which are then copied securely into the patient's secure e-vault for display in their portal. The pilot includes extracts in 18 topic areas, including labs, medication histories, and progress notes. The pilot also enables participants to delegate or grant access to selected portions of the PHR. Delegates and grantees must be registered in the system and access is managed by the patient from an interface within the system.

Although pilot sites were given flexibility in terms of some aspects of implementation, identity proofing and user authentication methods were standardized in order to meet required standards of "heavy proofing". All pilot sites required pilot participants to sign VA Release of Information forms and provide valid photo identification prior to being granted account access.

One potential concern in rolling out in-person authentication (IPA) throughout VA is the lack of on-site ROI staff to authenticate identity at some Community-Based Outpatient Clinics – particularly those in rural areas. VA has worked with its clinics to meet the needs of patients in these areas without requiring they travel to the nearest VA Medical Center for in-person authentication. VA Medical Centers that have satellite clinics are encouraged to ensure that staff members are available to perform IPA at the clinic.

Attention to users' needs is not limited to the initial IPA. VA has noted that pilot users often request support for retrieving username or password information in order to log in. As a complement to the initial account creation process, log-in support must likewise have systems and processes which protect account access. For example, although participants are able to submit requests for forgotten passwords through a web-based form, a centralized help desk team supported all pilot sites to ensure high levels of security. Requestors were required to provide a telephone number and respond to several questions in order to receive password information. If unable to meet these requirements, a password reset process was initiated instead.

For a PHR which includes a medication history and registration summary, initial in-person authentication is essential. This process is recommended whether or not the PHR currently contains sensitive or protected information, due to the potential for a basic PHR to be expanded with additional information requiring an additional level of security.

Over the several years that the My Health***e***Vet pilot has been conducted, no instances of inappropriate account access have been reported. This is likely due to the rigorous requirements for account access, including in-person authentication, and also as a result of the heavy emphasis user training places on security and the patient's responsibility in protecting username and password information. In-person authentication has been viewed by pilot participants as in their own best interest because it directly enforces the kind of security PHRs require.

The My Health***e***Vet Pilot has afforded VA an opportunity to gain practical experience with the demands and benefits of identity proofing and user authentication for personal health records.

Information in a PHR belongs to the patient, not to the organization providing the PHR system. In offering a PHR, a provider has entered a critical trust agreement with the health care consumer which must not be sacrificed for convenience. It is essential that health information remain private and secure, whether it is stored in an EHR, a PHR, or on paper. VA supports the development of guidelines and standards to ensure that authentication and identity management for PHR systems are handled consistently through out the health care community.

Thank you.