

# AHS Identification and Authentication Standard

---

Jack Green

10/8/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Identification and Authentication ( IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(8), IA-3, IA-4, IA-5, IA-5(1), IA-5(2), IA-5(3), IA-6, IA-7, IA-8) Controls.

## Revision History

Date	Version	Description	Author
	.99	Procedures received from HI and reviewed by Referentia	
10/8/2013	3.0	Procedures reviewed and adapted for VHC business processes and security requirements	Jack Green

### PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's (VHC) security control requirements for the Identification and Authorization (IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(8), IA-3, IA-4, IA-5, IA-5(1), IA-5(2), IA-5(3), IA-6, IA-7, IA-8) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

### SCOPE

The scope of this standard includes the VHC and its constituent systems only.

### STANDARD

#### **Identification and Authentication for VHC users**

1. The information system is configured to uniquely identify and authenticate all VHC employees on contractors.
  - Users must be uniquely identified and authenticated for all access. If an exception is required, it must be explicitly identified and documented to describe and justify the specific actions permitted without identification and authentication.
    - i. VHC users shall not share identification or authentication materials of any kind, nor shall any VHC user allow any other person to operate any VHC system by employing the user's identity.
    - ii. All user authentication materials shall be treated as sensitive material and shall carry a classification as high as the most sensitive data to which that user is granted access using that authenticator.
  - Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity.
2. In addition to identifying and authenticating users at the information system level (i.e., at log-on), identification and authentication mechanisms are to be employed at

the application level, when necessary, to provide increased security for the information system and the information it processes.

3. Authentication of user identities must be accomplished through the use of passwords, Personal Identification Numbers (PINs), tokens, biometrics, or in the case of multifactor authentication, some combination thereof.
4. An Electronic Authentication (“E-Authentication”) Risk Assessment must be conducted for any Agency information system that requires authentication over the Internet.
  - This E-Authentication Risk Assessment (ERA) must be conducted and used to determine the compliance requirements for access.
  - The ERA may be conducted as part a general risk assessment under the VHC Risk Assessment Procedures. It may also be a separate activity, in which case it must be informed by a general risk assessment for the information system.
  - The ERA process must identify potential impacts should proper authentication fail or should there be an authentication error.
    - i. These impacts are rated as low, moderate, or high risks.
  - The identified risks must then be mapped to the appropriate assurance level. There are four identity authentication assurance levels:
    - i. Level 1: Little or no confidence in the asserted identity’s validity.
    - ii. Level 2: Some confidence in the asserted identity’s validity.
    - iii. Level 3: High confidence in the asserted identity’s validity.
    - iv. Level 4: Very high confidence in the asserted identity’s validity.
  - The information system’s System Security Plan (SSP) must state if authentication is required. If authentication is not required, an explanation must be included.
  - Technologies for authentication must then be selected and implemented based on technical guidance provided in NIST SP 800-63, as amended.
  - Authenticators (e.g., passwords, randomly generated PINs, tokens, biometric, and other authenticators) and the selected technologies must comply with Level 2, 3, or 4 requirements.
  - Technology selection must be based first on technology standards or approved technologies within the VHC’s approved technology and security architecture.
    - i. If available technologies and mechanisms prove inadequate, alternatives that are consistent with NIST guidance may be proposed.
  - The guidance provided by NIST SP 800-63, must apply to both local and remote access to the information system.
    - i. Remote access connections must be both authenticated and authorized to be accepted.

- Validation must be conducted to ensure that the implemented system has met the required assurance level.

### **Device Identification and Authentication**

1. The information system must be configured to uniquely identify and authenticate end user operated devices (e.g. workstations, laptops, Voice over Internet Protocol (VoIP) phones, cell phones) and servers before establishing a connection.
2. The required strength of the device authentication mechanism must be determined by the security categorization of the information system as well as an assessment of risk incurred.
3. Host or device authentication must use only approved procedures, mechanisms, or protocols.
4. The procedures, mechanisms, or protocols used for device identification and authentication must be clearly documented, with diagrams, in the SSP.

### **Identifier Management**

1. Information system identifiers for users and devices must be selected such that the identifier uniquely identifies an individual or device.
  - Assignment of user identifiers must ensure that no two users have the same identifier.
  - A User Principal Name (UPN) must be implemented for each VHC issued smart card consisting of a unique user name and in accordance with VHC's e-mail standard naming convention, as appropriate.
    - i. Systems that do not implement smart card access must use a unique UPN username as an identifier.
  - User names must support the ready identification of employees (e.g., doe, john).
2. Authorization must be received from a designated organizational official to assign a user or device identifier.
  - A VHC sponsor shall issue user identifiers.
3. The user identifier must be assigned only to the intended party.
4. The device identifier must be assigned only to the intended device.
5. Inactive user identifiers must be:
  - Automatically disabled after 180 days of inactivity unless otherwise authorized by a supervisor.
  - Users can be allowed to self-activate disabled accounts within 180 after the account has been automatically disabled.
  - Accounts that have access to FTI data are automatically disabled after 90 days of inactivity.

6. User and device identifiers must not be reused for up to three years after the account has been deleted.
7. Longer periods may be specified as required for records retention purposes.
8. Default user names such as “sysadmin” or “administrator” must be changed before implementation of the information system or component (e.g. routers, switches, firewalls, printers, workstations, and servers).

### **Management of Authenticators**

1. The identity of the individual or device receiving an information system authenticator must be verified as part of the initial authenticator distribution.
2. Unique initial authenticator content must be established for user and device authenticators.
3. Authenticators for users and devices must have sufficient strength of mechanism for their intended use.
4. Administrative procedures must be established and implemented for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
  - If a user knows or suspects that their password has been compromised, they shall immediately:
    - i. Notify their immediate supervisor.
    - ii. Report a known or potential security breach to the DII help desk or to AHS IT Staff.
    - iii. Request the DII help desk to reset or change their password or if self-service password mechanisms are used, immediately change their own password.
5. Default content of authenticators (i.e., passwords provided for initial entry to a system) must be changed before implementation of the information system or component (e.g. routers, switches, firewalls, printers, workstations, servers).
  - The information system owner shall confirm that software and/or hardware upgrades, updates, and patches have not reinstated default passwords.
6. Authenticators must be changed or replaced periodically.
  - All newly assigned passwords must be changed the first time a user logs into the information system.
  - Passwords must be set to automatically expire in 60 days or sooner.
  - PIV (Smart Cards) certificates must be renewed every three (3) years.
7. The following minimum and maximum lifetime restrictions and re-use conditions must be adhered to regarding authenticators:
  - Passwords must have a minimum lifetime of 1 days and a maximum lifetime of 60 days.
    - i. Unless authorized by the information system owner, passwords cannot be changed in less than one (1) day.

- Password reuse is prohibited for 24 generations.
  - i. Password history must be set with a history of at least 24 passwords, so a user cannot quickly re-use a previous password.
- 8. Users shall take reasonable and specific measures to safeguard authenticators.
  - Users shall maintain possession of their individual authenticators, not loan or share authenticators with others, and report lost or compromised authenticators immediately to their supervisor and the VHC IT Staff as a security event.
  - Devices must be configured to safeguard authenticators (e.g., certificates, passwords).
- 9. For password-based and PIN based authentication, the information system must enforce the following:
  - Passwords must follow the VHC password standard.
    - i. Located at <http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec>
  - The PIN must be eight numerical digits at a minimum.
  - Prohibit passwords and PINs from being displayed when entered.
  - Encrypt passwords and PINs when stored and transmitted.

### **Cryptographic Module Authentication**

1. The information system must use mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

### **Identification and Authentication (Non-Organizational Users)**

1. The information system must be configured to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).
  - Non-organizational users are to be uniquely identified and authenticated for all access other than those accesses explicitly identified and documented as exceptions regarding permitted actions without identification and authentication.
2. A risk assessment must be used to determine the authentication needs of the organization.

### **IMPORTANT INFORMATION**

These procedures can be found at <http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec>