CA

126072 Security Requirements - Administrative Controls

(a)

Access Controls. A Demonstration Project Participant shall utilize identity management, authentication, and authorization mechanisms to ensure that only authorized users have access to information systems. (1) Identity Management (Internal). A Demonstration Project Participant shall establish policies and procedures to verify the identity of workforce members who will access the Participant's systems. A Demonstration Project Participant shall, at a minimum: (A) Verify that the individual is the one claimed by examination of various forms of state-issued picture identifications such as a driver's license or ID card, professional licenses in good standing from state or national certification boards, and other forms of identification issued by reliable bodies. The number and extent of such verification will be commensurate with the user's responsibilities and consistent with privileges they will be given (authorizations). (B) Issue a user identifier and an identity certificate and/or token (password, hard token, soft cryptographic token or one-time password device tokens, etc.), to the verified person, as appropriate to their level of authorization. (C) Be responsible for any health data access rights assigned to the authorized person based on their qualifications and role. (D) Manage all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. (2) Single Entity Authentication (Non-Federated).

A Demonstration Project Participant shall authenticate each authorized user's identity prior to providing access to IHI. (A) A Demonstration Project Participant shall assign a unique name and/or number for identifying and tracking user identity and implement procedures to verify that a person or entity seeking access to IHI is the one claimed. (B) A Demonstration Project Participant shall authenticate each user to the level of authorized access that complies with the Participant Agreement. (C) A Demonstration Project Participant shall authenticate users attempting to access IHI from an unsecured location or device, shall require NIST Level 3 authentication in which the data requester must establish two factors of authentication. [See NIST SP 800-63 Rev-1]

(1)

Identity Management (Internal). A Demonstration Project Participant shall establish policies and procedures to verify the identity of workforce members who will access the Participant's systems. A Demonstration Project Participant shall, at a minimum: (A) Verify that the individual is the one claimed by examination of various forms of state-issued picture identifications such as a driver's license or ID card, professional licenses in good standing from state or national certification boards, and other forms of identification issued by reliable bodies. The number and extent of such verification will be commensurate with the user's responsibilities and consistent with privileges they will be given (authorizations). (B) Issue a user identifier and an identity certificate and/or token (password, hard token, soft cryptographic token or one-time password device tokens, etc.), to the verified person, as appropriate to their level of authorization. (C) Be responsible for any health data access rights assigned to the authorized person based on their qualifications and role. (D) Manage all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

(A)

Verify that the individual is the one claimed by examination of various forms of state-issued picture identifications such as a driver's license or ID card, professional licenses in good standing from state or national certification boards, and other forms of identification issued by reliable bodies. The number and extent of such verification will be commensurate with the user's responsibilities and consistent with privileges they will be given (authorizations).

(B)

Issue a user identifier and an identity certificate and/or token (password, hard token, soft cryptographic token or one-time password device tokens, etc.), to the verified person, as appropriate to their level of authorization.

(C)

Be responsible for any health data access rights assigned to the authorized person based on their qualifications and role.

(D)

Manage all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

(2)

Single Entity Authentication (Non-Federated). A Demonstration Project Participant shall authenticate each authorized user's identity prior to providing access to IHI. (A) A Demonstration Project Participant shall assign a unique name and/or number for identifying and tracking user identity and implement procedures to verify that a person or entity seeking access to IHI is the one claimed. (B) A Demonstration Project Participant shall authenticate each user to the level of authorized access that complies with the Participant Agreement. (C) A Demonstration Project Participant shall authenticate users attempting to access IHI from an unsecured location or device, shall

require NIST Level 3 authentication in which the data requester must establish two factors of authentication. [See NIST SP 800-63 Rev-1]

(A)

A Demonstration Project Participant shall assign a unique name and/or number for identifying and tracking user identity and implement procedures to verify that a person or entity seeking access to IHI is the one claimed.

(B)

A Demonstration Project Participant shall authenticate each user to the level of authorized access that complies with the Participant Agreement.

(C)

A Demonstration Project Participant shall authenticate users attempting to access IHI from an unsecured location or device, shall require NIST Level 3 authentication in which the data requester must establish two factors of authentication. [See NIST SP 800-63 Rev-1]