حكومة دبي
GOVERNMENT OF DUBAI

هيئة الصحة بدبي
DUBAI HEALTH AUTHORITY

نابض
NABIDH

Unifying Dubai's Healthcare

Policies and Standards

September 2020 (v1.0)

SECTION 6: Identity Management Policy

1. Purpose:

1.1. To define the identity management requirements for a secure system level access and to ensure systems and individuals interacting with NABIDH are known through a process of reliable security identification by incorporating identifiers and its authenticators.

1.2. To establish the categories of users and their respective identity authentication parameters within the NABIDH platform.

2. Scope/ Applicability

2.1. The scope of this document is the specification for audit requirements for implementation of the NABIDH platform among DHA licensed healthcare providers in the Emirate of Dubai.

2.2. This policy applies to NABIDH, and to all individuals and Healthcare facilities that have access to NABIDH managed Health Information, including:

2.2.1. DHA and their Business Associates or any subcontractors, who is responsible for oversight of NABIDH platform.

2.2.2. Public Health and their Business Associates or any subcontractors who is responsible for exchange of PHI.

2.2.3. NABIDH and their Business Associates or any subcontractors who is responsible for exchange of PHI.

2.2.4. HealthCare Facilities, their Business Associates, or any subcontractors who is responsible for submission, collection and use of PHI.

2.2.5. Subject of Care or the Subject of Care Agent who is responsible for providing appropriate consent to their data.

3. Policy Statement

3.1. Dubai Health Authority shall:

3.1.1. Develop and implement standards and guidance on identity authentication and management for users of the NABIDH platform in accordance with all applicable Laws and DHA Regulations.

3.1.2. Continuously improve related regulatory and compliance frameworks.

3.2. NABIDH shall:

3.2.1. Define specifications that qualify as National Identifiers to authenticate the various categories of users for the NABIDH platform

3.2.2. Assume full authority for granting access privileges to users, based on the authentication of identities by Healthcare Facility for each of its approved users.

3.2.3. Identify entities for verification and management of digital certificates for NABIDH users from Healthcare Facility and their Business Associate.

3.2.4. Ensure that the identity of individual users accessing the NABIDH system shall be subject to identity verification for the issuance of access credentials.

3.2.5. Ensure that federated identity proofs be applied to authenticate users to the NABIDH platform on a case by case basis.

3.2.6. Define the requirements for Proof of Identity for individuals as follows:

a. Identity Proofing for all individual users shall include a face-to-face verification of the individual's identity.

b. Identity proofing for all individual users shall require a valid government issued photographic identification. The National Emirates ID shall be the primary identification document; however, passport, driver's license, DHA employee ID or Residency Permit for Residents or a government recognized biometric identification can be considered in absence of the National Emirates ID.

c. For Subject of Care, the identity proofing will be conducted at the Healthcare Facility with a valid government issued photographic identification. The primary identification document shall be the updated National Emirates ID. However, valid passport, driver's license or Residency Permit for Residents or other government recognized biometric identification shall be accepted in the absence of the National Emirates ID. The Emirates National ID shall be duly updated as per validity in the NABIDH platform. Antecedent Data (e.g. from a prior health visit) may be used as the face-to-face verification of the individual’s identity.

d. For Subject of Care agent, additional proofing shall be provided indicating authorization to act on behalf of the Subject of Care for access to NABIDH.

e. Identity Proofing for Regulated Health Professional requires evidence of a current healthcare license issued by the Dubai Health Authority in addition to the Identity Proofing requirements that apply to all individuals.

f. Identity Proofing for Non-Regulated Health Professionals shall require verification of employee ID or letter from employer on employer letterhead indicating current employment status in addition to the Identity Proofing requirements that apply to all individuals.

g. Identity Proofing of a Sponsored Healthcare Provider shall require a letter from a Regulated Healthcare professional or authorized

h. Representative of a sponsoring regulated health organization to establish that they are active in their healthcare community OR evidence of current credentials issued by the Dubai Health Authority in addition to the Identity Proofing requirements that apply to all individuals.

i. For other users (e.g. researchers), antecedent data may be used to provide limited access to NABIDH platform.

j. Be informed on Healthcare or non-healthcare professionals who are terminated from Healthcare Facility and determine the termination of access to those users on case-to-case basis. An acknowledgment of receipt of notification on employee termination should be issued upon receipt.

3.2.7. Be informed by the Healthcare Facility upon individual user's role modification for any employee who has been issued an individual identity credential to access NABIDH. An acknowledgment of receipt of notification on employee role modification should be issued upon receipt.

3.2.8. Establish defined requirements for Proof of Identity for Healthcare Facility and Organization's systems as follows:

a. Verification by an individual identified by the organization as authorized to provide such attestation.

b. A letter on the entity letterhead signed by a corporate officer shall identify the representative of the entity, authorized to validate and request organization or device certificates on behalf of the entity that will be used for the provision of Healthcare Facility certificates.

c. The Organization responsible shall provide proof of a current license to conduct the healthcare or healthcare associated business, a valid commercial registration document by a nationally recognized government entity.

3.2.9. Ensure Healthcare Facility agreements include the requirement to protect their identity credential.

3.2.10. Establish a process for Healthcare Facility to notify the NABIDH Privacy and Security officer, if their digital identity is lost, stolen, or otherwise known to be compromised. Further, on, a revocation request shall be launched along with a request for a new digital identity. Refer to NABIDH Breach Notification Policy for reporting.

3.2.11. Maintain a log-list of all individuals and Healthcare Facility along with their respective identity authentication documents that have access to the NABIDH system along with the data contribution endpoint infrastructure. The list must include the following:

a. The ID credentials.

b. Person or information system's details: full name, department, and location, and contact information (email and telephone number, where available)

c. Identity proofing documents

3.3. <u>All HealthCare Facilities shall:</u>

3.3.1. Implement initial identity-proofing procedures, in accordance with the Identity Management Policy, that requires Authorized Users to provide identifying materials and information upon application for access to the NABIDH Platform.

3.3.2. Be responsible for authenticating each individual authorized User's identity prior to granting access to NABIDH Platform.

3.3.3. Assign a unique name and/or number to all Authorized Users within the healthcare facility that access the NABIDH Platform for identifying and tracking user identity.

3.3.4. Be subject to verification by NABIDH for the issuance of identity credentials.

3.3.5. Be subject to verification by NABIDH for utilization of digital certificates.

3.3.6. Be responsible for identity proofing for all Subject of Care. The identity proofing will be conducted at the Healthcare Facility with a valid government issued photographic identification.

3.3.7. For Subject of Care agent, additional proofing shall be provided indicating authorization to act on behalf of the Subject of Care for access to NABIDH platform.

3.3.8. Ensure procedures for account revocation upon employee termination are implemented:

a. Notification to NABIDH shall be issued at least two days prior to the last date of service termination.

b. Receive an acknowledgment of notification from NABIDH.

c. Account revocation by the Healthcare Facility and NABIDH should be set in the NABIDH platform to ensure access revocation within two business days after receiving notification.

3.3.9. Ensure procedures for account revocation upon employee severance due to misuse of PHI data are implemented in alignment with the NABIDH Breach Notification Policy (Section 3).

a. Notification to Sheryan and NABIDH shall be issued with immediate effect for healthcare professionals.

b. Notification to NABIDH shall be issued on immediate effect for non-healthcare professionals.

c. Receive and acknowledgment of receipt of notification.

d. Account revocation by the Healthcare Facility and NABIDH should be implemented with immediate effect after the receipt of notification.

3.3.10. Ensure procedures for account update upon employee role modification for any employee who has been issued an individual identity credential to access NABIDH are implemented:

a. Notification to NABIDH should be issued within two business days.

b. Receive an acknowledgment of receipt of notification should be issued upon receipt.

c. Account update by the Healthcare Facility and NABIDH should be implemented within two business days after notification

3.3.11. Ensure to notify the NABIDH Privacy and Security officer, if their digital identity is lost, stolen, or otherwise known to be compromised. Refer to NABIDH Breach Notification Policy for reporting (Section 3).

3.4. <u>The Subject of Care or the Subject of Care Agent shall:</u>

3.4.1. Provide their identity proofing to HealthCare Facility, in accordance with NABIDH Identity Management Policy.

3.4.2. Be subject to all identity verification procedures implemented by NABIDH for the issuance of identity credentials.

Contact Us

Still have questions?

For more information on NABIDH, please reach out through the following channels:

800 DHA (800 342)	info@dha.gov.ae	https://nabidh.ae

This document was last updated on **01 Sep 2020**