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 7: Authentication and Authorization policy

1. Purpose:

1.1. To allow only authorized users and certified applications to access information through NABIDH.

1.2. To limit exchange of information to minimum number of individuals necessary for accomplishing the intended purpose of the exchange.

1.3. To embed confidence in the privacy of subject of care Health Information as it is transferred across the health system to meet their needs.

2. Scope:

This policy applies to all users accessing and using NABIDH including:

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

2.2. NABIDH and their Business Associates or any subcontractors who are responsible for exchange of subject of care Health Information.

2.3. HealthCare Facilities and their Business Associates or any subcontractors who are responsible for submission, collection and use of subject of care Health Information.

2.4. 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. Oversee the implementation of further policies, standards, and guidelines related to NABIDH Authentication and Authorization as necessary in accordance with applicable Laws and DHA Regulations.

3.2. NABIDH Shall:

3.2.1. Maintain Authentication and Authorization standards and protocols that are compliant with Applicable Laws, DHA regulations and DHA Health Information Security Standard (HISS) that all member participants must adhere to.

3.2.2. Users shall be authenticated against identity access management system.

3.2.3. Verify the user identity, role, and affiliation at the time of logon to the system. If any of these has been revoked or has expired, access shall be denied.

3.2.4. Suspend user access if the approved users do not use their access for 90 days.

3.2.5. Provide access once authorization procedures have been indicated by the relevant Healthcare Facility as being completed and list of Authorized Users has been received.

3.2.6. Authorization of users shall be role based taking into account an individual's job function and information required to carry out their role.

3.2.7. Define and establish categories of Authorized Users and access levels that will ensure that an end user can access types of information only if they are permitted to do so.

3.2.8. Categorize and define in the Participation Agreement the types of Subject of care Health Information that each category of Authorized User may access and the purposes for which they may access it.

3.2.9. Ensure that NABIDH system remote access by individual users shall require secure authentication process.

3.2.10. Ensure that all HIE Nodes exchanging Personal Health Information shall implement a node authentication mechanism compliant with security standards (Section 8).

3.2.11. The user sessions of the HIE node should be automatically logged off after no more than 15 minutes of inactivity.

3.2.12. In the case of suspected breach or virus attack or incidents, NABIDH has the right to turn off access to the node to avoid any further breach or damage.

3.2.13. Support Emergency Access to all care providers accessing the NABIDH as a break-glass with audit and review of these actions, in accordance with the Audit Policy. Notification should be sent to the subject of care and to the Data Privacy and Security officer.

3.2.14. Maintain a Registry of Participants within the NABIDH that may include primary contact information of registered users,

roles/privilege information, and identity attributes of providers, organizations, and systems.

3.2.15. Ensure NABIDH is capable of identifying all users who have accessed, or modified a given subject of care/person's record(s) over a given period of time.

3.2.16. Conduct periodic access reviews including applications, infrastructure, Data centre and third parties.

3.3. HealthCare Facilities Shall:

3.3.1. Comply with all current applicable laws and regulations such as UAE ICT Law, DHA regulations, Federal and Local Laws, etc. regarding Authentication and Authorization of users.

3.3.2. Ensure compliance of all systems and processes using NABIDH with the DHA HISS.

3.3.3. Prior to providing access to NABIDH platform, verify and authenticate the identity of their Authorized Users within the scope of this policy to access Data through NABIDH (Section 6).

3.3.4. Authenticate the identity of Authorized Users through physical and digital identity checks before granting access to NABIDH. The NABIDH shall require unique identification of the individuals (Healthcare Facility identifiers, employees, care providers, subjects of care, subjects of care agents), systems (HIE node, HIE system, or the Application), and Organizations accessing the information in the NABIDH.

3.3.5. Ensure that the level of access granted is appropriate to the business purposes of Authorized Users.

3.3.6. Ensure that each authorized user shall complete training prior to activation of access to NABIDH and these authorized users shall undergo refresher training on annual basis.

3.3.7. Develop, maintain and implement relevant access control policies and procedures. Each Participant will be responsible for designating its authorized users and establishing their level of access based on their job function.

3.3.8. Immediately terminate the user-access privileges of permanent or temporary employee or third-party contractor who is a registered user of system and who has access to NABIDH upon termination of their employment with the organization.

3.3.9. Notify Sheryan and NABIDH when Healthcare professionals are terminated from Healthcare Facility for misuse of Personal Health Information.

3.3.10. Notify NABIDH when non-Healthcare professionals are terminated from Healthcare Facility for misuse of Health Information.

3.3.11. Assert secure authentication process for remote access to NABIDH clinician portal (from outside of the physical control of the organization).

3.4. Subject of Care Shall:

3.4.1. Follow authentication process to access subject of care portal.

3.4.2. Refrain from disclosing portal passwords to any other person.

3.4.3. Inform NABIDH administrator or Healthcare Facilities administrators if the subject of care portal account is hacked or compromised.

3.4.4. Be responsible and liable for all actions including information retrieval or communication performed on subject of care portal.

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**