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 4: Audit Policy

1. Purpose:

1.1. To define compliance and audit requirements for the NABIDH Platform.

1.2. To assure effectiveness of implemented information security controls and prevent violations and breaches as per the laws, policies, or controls within the UAE.

1.3. To provide guidance in identifying and preventing unauthorized access to PHI within the NABIDH system and to comply with relevant privacy requirements.

1.4. To define the roles and responsibilities of all the relevant participants within the NABIDH system

1.5. To have an effective auditing process that ensures confidentiality of PHI within NABIDH.

1.6. To define the frequency and specifications of maintaining Audit Logs for maintaining Audit Logs for documenting all the access to and receipt of PHI through the NABIDH system.

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 PHI, including:

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

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

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

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

3. Policy Statement:

3.1. Dubai Health Authority Shall:

3.1.1. Develop and implement standards and guidelines on auditing the performance and security features of the NABIDH platform in accordance with all relevant legislative statutory, regulatory, and contractual requirements.

3.1.2. Continuously improve the related regulatory and compliance frameworks.

3.1.3. Perform annual audits on the NABIDH platform and their appointed third-party vendor to ensure compliance with all applicable Laws and Policies.

3.2. NABIDH shall:

3.2.1. Implement technical processes that accurately record all activities related to access, creation, modification, disclosure and deletion of electronic PHI that facilitates the auditing process of the NABIDH Platform as per the NABIDH Audit Policy and standards.

3.2.2. Assure all HEALTHCARE FACILITY node and NABIDH systems shall be configured to generate logs of all events (e.g. login, logoff, access events, denial events, etc.) as supported by installed products to enable further investigation and traceability.

3.2.3. Audit the compliance with applicable legislative, regulatory and contractual requirements related to intellectual property rights and use of copyrighted/licensed materials, software or applications.

3.2.4. Perform regular audit on the compliance of information processing and procedures relating to the security policies, standards and any other security requirements.

3.2.5. Perform a risk assessment for all information systems periodically, or following significant business or technology changes to systems, contract renewals, extensions and/or vendor changes.

3.2.6. Undertake an independent review of the Healthcare Facility approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) at planned intervals or when significant changes occur.

3.2.7. Conduct reviews and reports on NABIDH information assets assurance processes regarding security matters (e.g., incidents,

responses, issues, risks). This may include undertaking specialist internal/external audits of their environments and taking appropriate action based on findings and recommendations.

3.2.8. Establish defined responsibilities to the Health Informatics and Smart Health Department (HISH) for periodically auditing of the performance and compliance for the NABIDH platform. Health Informatics and Smart Health Department (HISH) shall be responsible for recommending the frequency of the audits to be performed, the specific controls to be audited and notifying participants and determining the sample size for each audit. The department shall also review the results of the audits and any corrective action to be taken as a result of problems uncovered during the audits and make recommendations as to whether the specified corrective action should be accepted.

3.2.9. Define the audit log to include specific audit functions including but not limited to:

a. Review of system administrator authorizations and activity.
b. Review of network intrusion detection system activity logs.
c. Review of physical access to data centres.
d. Procedures for follow-up on suspicious activity, such as indications of possible privacy or security breaches.
e. Other review of technical, physical, and administrative safeguards as established by the policies of the organization

3.2.10. Ensure audit logs are either in human readable format or translatable by some easy to use tool to be in human readable format.

3.2.11. Ensure audit logs are retained for Three (3) years, the same duration as the retention time required of NABIDH managed PHI.

3.2.12. Ensure audit log review of the systems shall include but not limited to software applications, networks, servers, firewalls and other network hardware and software:

a. All system logs shall be reviewed by the nominated designee from the respective HealthCare Facility.
b. The generated audit logs shall be reviewed on a regular basis based on audit criteria developed in advance, at least quarterly, in order to detect improper use of the PHI.
c. All anomalies shall be documented and appropriate mitigating action shall be taken and documented.
d. All system audit logs and evidence shall be provided to Health Informatics and Smart Health Department (HISHD) upon request for any investigation.

3.2.13. Ensure privacy and security audit review shall support inquiry by stakeholders and users.

3.2.14. Ensure external audits of the NABIDH shall be conducted at least annually as a minimum requirement and when any major system or business change occurs. Comprehensive audit procedures should be developed, documented, and made available. The external audit shall include:

a. The generation of a compliance audit findings report and documentation of any identified deficiency that needs to be addressed in order of priority.

3.2.15. Ensure audit record repository system includes the following but not limited to:

a. List all users that accessed or modified a given Subject of Care's information over a period of time.
b. List all Subjects of Care whose Health Information was accessed by a given user/system over a given period of time,
c. List of all break glass events,
d. List all access events where the user is not listed as a provider in any subject of care records, and
e. List events that request information marked as sensitive.

3.2.16. A valid date, time, and stamp shall be used for data authentication purposes.

a. All HIE nodes exchanging PHI shall implement the time synchronization mechanism specified by NABIDH to assure that timestamps and audit logs are synchronized.

3.2.17. Ensure that the audit logs repository is secured in accordance with the NABIDH information security standard (Section 8). Access to system audit log analysing tools and audit logs shall be safeguarded to prevent misuse or compromise.

3.2.18. Ensure that NABIDH audit logs access are restricted only to the respective designated assignees from Healthcare Facility and NABIDH.

3.3. All Healthcare Facilities shall:

3.3.1. Implement technical processes and policies for accurate, timely, and secure recording of activities related to access, creation, modification, disclosure, and deletion of electronic PHI that facilitates the auditing process in compliance with the NABIDH Platform and this policy.

3.3.2. Successfully complete all required audit testing for all applications by NABIDH users. Applications that have not yet completed this testing will be considered on a case-by-case basis.

3.3.3. Log all transactions of clinical data within the NABIDH Platform to support periodic auditing and to have all activities logged locally, and maintained in a persistent database.

3.3.4. Ensure that log files are not altered, in order to prevent sophisticated attackers from removing traces of their work. Such logs must not contain the full record being transmitted, so that the logs themselves do not become an alternate target for attackers looking for clinical information.

3.3.5. Ensure that, as part of log-in monitoring, an audit log shall be created and maintained to record user logs on to the NABIDH platform. This should include all attempted and failed logons.

3.3.6. Ensure that for the purposes of information use or disclosure, the audit log shall include the following documentation of the request to access to the PHI through the NABIDH platform:

a. The date and time of the request.
b. Location of access.
c. The reason for the request.
d. A description of the information requested, including the data accessed, the data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to another party.
e. Whether the request was performed as a “break glass”.
f. Whether the requested information was marked as sensitive PHI.
g. Whether the access is made by a privileged account user.
h. The ID of person/system requesting the access to PHI.
i. The ID of the person/system generating response for PHI access requests.

3.3.7. Be responsible to recommended corrective actions to NABIDH in response to problems uncovered during the audits and implement the approved corrective actions and along with additional corrective actions recommended by the NABIDH privacy and security committee as a result of audit reviews.

3.3.8. Have the ability to generate an electronic access report summary of PHI exchanged for all applications within the NABIDH.

a. This capability shall be demonstrated when integrating the Healthcare Facility Node to the NABIDH system

b. Testing of this capability shall be conducted by NABIDH.

c. The Healthcare Facility should be able to audit all access to PHI that is stored locally.

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**