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 3: Incident Management and Breach Notification policy

1. Purpose:

1.1. To ensure appropriate tools, processes and procedures are in place to detect report and manage incidents and breach of protected PHI within the NABIDH Platform and for participating organizations.

1.2. To establish roles and responsibilities for individuals and HealthCare Facilities that have access to NABIDH managed PHI in order to prevent such breach within the NABIDH Platform.

2. Scope/ Applicability:

2.1. The scope of this document is the implementation of breach management for 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 or Their Business Associates or any subcontractors who is responsible for submission, collection and use of PHI.

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

3. Policy statement:

3.1. Dubai Health Authority shall:

3.1.1. Develop and oversee the implementation of policies, standards, and guidelines related to the protection of PHI and specify the requirement for identification, notification and management of incidents and breach of information managed by NABIDH in accordance with all applicable UAE laws and DHA regulations.

3.1.2. Be held responsible for unauthorized disclosure of information accessed via the NABIDH Platform by their staff.

3.1.3. Enforce continuous improvements related to regulatory and compliance frameworks.

3.2. NABIDH shall:

3.2.1. Establish processes and responsibilities for management of incidents in compliance with the Health Information Security Standards to protect and prevent breach of Health Information within the NABIDH Platform.

3.2.2. Implement appropriate technical and organizational measures to protect against accidental, negligent or unlawful loss, disclosure or access to PHI, particularly in the context of processing or transfer of PHI to recipients.

3.2.3. Ensure all Healthcare Facility and individual users are made aware of their responsibilities for reporting information security incidents/ events/weaknesses, including whom to report and the location of the applicable policies/procedures.

3.2.4. Perform vulnerability assessments of the security measure of NABIDH to determine where weaknesses may exist and improvements can be made.

3.2.5. Notify vendors and/or certifying bodies of failures in system security controls.

3.2.6. Notify all affected parties and stakeholders of the security incident and possible consequences e.g. loss of data integrity.

3.2.7. Establish and publish a process for incident logging, response, handling, escalation and recovery to inform and guide those required or eligible to file reportable events and incidents. This process will take into account the privacy of information of Subject of Care involved in the reportable events and incidents.

3.2.8. Establish a common point of reporting for significant information security incidents to Nabidh@dha.gov.ae

3.2.9. Appoint the NABIDH Information Security Officer with defined roles and responsibilities for management of incidents.

3.2.10. Ensure NABIDH Information Security Officer Audits and monitors the incidents of breach on a regular basis within NABIDH and HealthCare Facility.

3.2.11. Develop quarterly summary report of all reported events and incidents within the NABIDH platform.

3.2.12. Ensure NABIDH Information Security Officer contacts NABIDH users and Healthcare Facility that have access to the NABIDH, to review any suspicious activity. In case of an incident or reportable event, NABIDH Information Security Officer and Healthcare Facility Information

Security Officer shall immediately investigate the suspicious activity and generate a report of the event.

3.2.13. Notify the concerned Healthcare Facility Information security officer(s) or designee and the Subject of Care in the event that a breach is identified and investigated by the NABIDH Information Security Officer.

3.2.14. Ensure NABIDH Information Security Officer receiving the Incident report or reportable event Report shall log the incident or reportable event.

3.2.15. The NABIDH Information Security Officer shall acknowledge the receipt of the Reportable Event Report to the person or system, filing it within 48 hours or two (2) business working days, and inform the affected Healthcare Facility Information Security Officer or designee of the event, if they do not already have knowledge of it, and subsequently begin a review of the event.

3.2.16. Ensure that, upon receipt of a reportable event or incident, it shall be reviewed by the NABIDH Information Security Officer to determine whether an investigation is required.

3.2.17. Facilitate protection of PHI, collection of evidence related to the reported incident and identity involving staff disciplinary or legal action.

3.2.18. Identify the need to revoke Healthcare Facility and/or individual users' accesses to NABIDH and as a result of the reported incident, develop measures to handle duress situations on a case to case basis.

3.2.19. Ensure that all relevant incidents and reportable events shall be investigated based on the incident priority matrix to identify the root cause within a maximum of 30 days and submit a final written report to the concerned parties (Appendix 4).

3.2.20. Determine that no further action is needed; this shall be communicated to the originator of the incident or reportable event, thus terminating the review process. Such decisions are subject to review through internal or external audits, based on the organizational framework of NABIDH.

3.2.21. Ensure that time and scope constraints for the investigation on the incident or reportable event of a confirmed breach will be a maximum of thirty (30) days, followed by mitigation actions taken within 180 days.

3.2.22. Ensure that in the case of an imminent threat to data security within NABIDH, the NABIDH Information Security Officer shall take immediate actions to secure the data, which could lead to suspension of individual and Healthcare Facility user(s) access or account revocation.

3.2.23. Suspension of access privileges and/or account revocation may be enforced until the source of incident has been mitigated locally or possibly permanently as considered on a case-by-case basis.

3.2.24. Healthcare Facility shall fully cooperate with the NABIDH Information Security Officer in identification and mitigation of the threat that could result in a breach event.

3.2.25. Once the review is done, the NABIDH Information Security Officer shall determine whether a violation of privacy and security policies, procedures, or relevant law has occurred.

3.2.26. Notify DHA of any breach as soon as reasonably practicable after determining that a breach occurred, but in any event within 48 hours.

3.2.27. An incident Investigation Report shall be prepared, documenting the facts gathered from the review, event mitigations, and measures to be taken to prevent recurrence of such an event.

a. The Investigation Report shall be completed within thirty (30) calendar days of receiving the reportable event Report by NABIDH.
b. This timeframe MAY be extended for another 30 days on a case by case basis. This extension in the Breach Investigation Report shall be communicated to the originator of the Reportable Event Report or incident.
c. This report shall be retained for a minimum of twenty five (25) years, in compliance with DHA guidelines for managing health records.

3.2.28. When a Reportable Event is established as a privacy breach, NABIDH shall notify the HealthCare Facility, whose information was subject to unauthorized acquisition, access, use, or disclosure, no later than 48 hours or 2 business working days following the discovery of the breach.

3.2.29. When a breach occurs at the HealthCare Facility, any required public notification is the responsibility of the HealthCare Facility. If a breach occurs at NABIDH level, then, it's the responsibility of NABIDH to report the breach. In some situations, (e.g. where it is determined that it is important for the communication to be initiated by the healthcare provider organization rather than NABIDH), NABIDH shall to report to the HealthCare Facility, which shall in turn make any required public notifications. Such notification shall be made within thirty (30) days following discovery of the breach.

3.2.30. Ensure the notification to the Subject(s) of care shall contain, to the extent possible, the following:

a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

b. A description of the types of PHI that were involved in the breach (such as full name, national identification number, date of birth, home address, etc.). The steps individuals should take to protect themselves from potential harm resulting from the breach.

c. A brief description of what Healthcare Facility and NABIDH are doing to further investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.

d. Contact procedures for individuals to ask questions or learn additional information, which shall include a telephone number, an email address, a web site, or postal address.

e. Procedure to report a petition with DHA in case the subject(s) of care are unhappy with the results of the investigation and corresponding actions.

3.2.31. Ensure breaches involving a single Individual and breaches involving small numbers of individuals should be reported to the Subject of Care involved in the breach. Breaches affecting large numbers of individuals, typically more than five hundred and involving continuous risk should be reported to DHA. The NABIDH Information Security Officer shall make such decision in collaboration with NABIDH and DHA.

3.2.32. Ensure NABIDH Information Security Officer and the Healthcare Facility Information Security Officer(s) involved in the incident shall collaborate to develop, approve, and implement the mitigation plan to proactively prevent a similar breach from re-occurring.

3.2.33. Ensure that the NABIDH Information Security Officer shall review existing policy for necessary changes to avoid any further breaches.

3.2.34. Ensure that the NABIDH Information Security Officer shall conduct the required educational campaign within NABIDH and associated organizations as necessary to educate employees on how to avoid further breaches.

3.2.35. Ensure that the NABIDH Information Security Officer shall take appropriate disciplinary action regarding the individual responsible for the breach, in accordance with the Information Technology Law (ICT) Law (article 25).

3.2.36. NABIDH Privacy & Security officer has to report the information security incidents to the DHA Information Security Office.

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

3.3.1. Oblige to follow the NABIDH breach notification policy for all incidents and reportable events involving the breach of protected PHI within the NABIDH Platform.

3.3.2. Develop and implement internal policies and procedures regarding beaches, which describe the different mechanisms for reacting to such breaches based on the priority of incidents (Appendix 4), and must include an internal notification process and a root cause analysis.

3.3.3. Update and provide periodic trainings for Authorized Users within the Healthcare Facility regarding identifying and notifying breaches within the NABIDH platform.

3.3.4. Be held responsible for unauthorized disclosure of information accessed via the NABIDH Platform by their staff.

3.3.5. Allocate an Information Security Officer(s) or appropriate designee to audit and monitor the security measures and review any suspicious activity on a monthly basis.

3.3.6. Ensure the Healthcare Facility Information Security Officer(s) or designee shall fully cooperate with the NABIDH Information Security Officer in identification, investigation, assessment and mitigation of reportable events involving their Healthcare Facility and/or Subject of care.

3.3.7. Ensure the Healthcare Facility Information Security Officer(s) or designated person shall communicate all incidents and reportable event and reviews to the concerned authorities in NABIDH, within (48 hours) of the discovery of an incident in accordance with the Breach Notification Policy.

3.3.8. Notify subject of cares affected, and any applicable regulatory agencies as required in accordance with Applicable Laws.

3.3.9. Ensure the Healthcare Facility Information Security Officer(s) or designee shall conduct internal review of the incidents and also cooperate with the NABIDH Information Security Officer in investigation, assessment and mitigation of reportable events involving their Healthcare Facility and/or Subject of care.

3.3.10. Ensure that the Healthcare Facility Information Security Officer is responsible for preventing further breaches and incidents within the Healthcare Facility.

3.3.11. Ensure that the Healthcare Facility Information Security Officer shall review existing policy for necessary changes to avoid any further breaches.

3.4. The Subject of Care or the Subject of Care Agent shall:

3.4.1. Ensure in the case of a suspected breach, identified by the Subject of Care, he or she can initiate a notification of incident or reportable events using the complaint form or other means, which shall be accepted by the Healthcare Facility Information Security Officer and further can request an investigation as per the Breach Notification Policy. This incident shall be reported to the NABIDH Information Security Officer.

3.4.2. Direct the request to the NABIDH Information Security Officer, if the results of investigation from the Healthcare Facility is considered unsatisfactory by the complainant.

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**