

PARTNERSHIP FOR ACHIEVING TOTAL HEALTH

Greater New Orleans Health Information Exchange

Section: HIPAA		Subject: BREACH NOTIFICATION POLICY	
Controls Addressed:	Regulations	Controls	
	Security (A)	45 CFR 164.308(a)(1)	
Applies to: <input checked="" type="checkbox"/> LPHI <input type="checkbox"/> PATH <input type="checkbox"/> Business Partner		Effective from: 9-10-2015	Revised on: 10-22-2019
Approved: 6/2019,11/2019			
Page 1 of 6			

I. PURPOSE

The Breach Notification policy aims to ensure that the Greater New Orleans Health Information Exchange (GNOHIE) and Participating Organizations and Members comply with applicable law to make the appropriate notifications and disclosures in the event of a breach. Establishing protocols related to breach notification of the protected health information (PHI) is essential to build trust among members and remain in compliance with the law.

The Partnership for Achieving Total Health (PATH), as the primary project manager and fiduciary agent of GNOHIE, is responsible for guarding against the inappropriate use and disclosure of protected health information (PHI). This policy describes PATH’s and GNOHIE Participating Organizations’ and Members’ responsibilities as they relate to breach notification in the event that PHI data has been breached, accessed by an unauthorized user/s, or used inappropriately.

II. SCOPE

This policy applies to GNOHIE and data stored within GNOHIE.

III. POLICY STATEMENT

A. RESPONSIBILITY FOR IDENTIFICATION AND REPORTING OF BREACHES

1. Internal Reports.

- i. Employees, agents, and independent contractors of PATH must report any breach, as soon as is practicable upon breach discovery, to the Security Officer assigned by PATH.
- ii. Once the Security Officer is notified of the breach, the requirements set forth in Section B below (Notification to Individuals and Participating Organizations/Members) will apply.

2. GNOHIE Participating Organizations and Members. Participating Organizations and Members, including their employees, agents and independent contractors, shall notify the GNOHIE Security Officer as soon as possible, in a timeframe not to exceed twenty-four (24) hours of breach discovery of the GNOHIE system data, and must continue to provide such information, within twenty four (24) hours after it becomes available, that PATH is required to provide to affected individuals, Participating Organizations, Members, or the Government.

3. Business Associates. PATH's, Participating Organizations', and Members' business associate agreements shall specify that business associates and their employees, agents and independent contractors will report breaches (other than breaches affecting only PHI of the Participating Organization and/or Member) to the GNOHIE Security Officer as soon as possible, in a timeframe not to exceed twenty-four (24) hours of breach discovery of the GNOHIE system data, and must continue to provide such information, within twenty four (24) hours after it becomes available, that PATH is required to provide to affected individuals, Participating Organizations, Members, or the Government.

4. Notification Process. When notifying the GNOHIE Security Officer of a breach, GNOHIE Participating Organizations, Members, business associates, and all associated employees, agents and independent contractors shall use the following process:

- i. Notification shall be in writing.
- ii. Notification shall contain the following content:
 - 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 whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
 - c. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
 - d. Any steps GNOHIE Participating Organizations, Members, business associates, and associated agents and independent contractors, as applicable, are taking to notify individuals who are their patients and that may otherwise be required by law or advisable to protect themselves and their patients from potential harm resulting from the breach;
 - e. A brief description of what GNOHIE Participating Organizations, Members, business associates, and associated agents and independent contractors, as applicable, are doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- iii. Notification to the Security Officer should be sent to the following address in a secure manner that will protect the confidentiality of the information and will ensure that delivery is made within the twenty-four (24) time period as required in section A(2) and A(3) above:

1515 Poydras St., Suite 1200
New Orleans, LA 70112

5. PATH is considered to have been notified of the breach on the date of receipt of the notification issued under the requirements in Section A(4) above, provided that such notice is received prior to close of business. If notification is received after close of business, PATH will be considered to have been notified of the breach on the next business day.

B. NOTIFICATION TO INDIVIDUALS AND PARTICIPATING ORGANIZATIONS / MEMBERS

1. Mandatory Notification. All affected individuals must be notified in the event of a breach.

2. Responsibility for Notification.

- i. Participating Organizations and Members will be responsible for providing notification to affected individual(s) in cases in which the breach originated with the Participating Organization or Member, or any Participating Organization or Member business associate.
- ii. In the case of a central event affecting the GNOHIE but not associated with any one Participating Organization, Member, or Participating Organization or Member business associate interaction with the GNOHIE, PATH will coordinate with the affected Participating Organizations or Members on the dissemination of the notification to the affected individual(s).

3. Timing of Notification.

- i. PATH shall notify affected Participating Organizations and/or Members without unreasonable delay but in no case later than 24 hours after PATH is notified of a breach (according to Section A(5) above) affecting PHI of the Participating Organization and/or Member.
- ii. If a Participating Organization or Member is required to notify affected individuals, the Participating Organization or Member will do so without unreasonable delay, but in no case later than 60 days after breach discovery.
- iii. If PATH is required to notify affected individuals, PATH will do so without unreasonable delay, but in no case later than 60 days after breach discovery.

4. Content of Notification. The party responsible for the notification to patients, either the Participating Organization or Member or PATH, shall include in the Notification to the extent possible, in plain language:

- i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- ii. A description of the types of PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- iii. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- iv. Any steps PATH and/or Participating Organization or Member is taking to notify individuals who are their patients and that may otherwise be required by law or advisable to protect themselves and their patients from potential harm resulting from the breach;
- v. A brief description of what PATH and/or the Participating Organization or Member is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- vi. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

5. Delivery of Notification.

- i. All notices to affected individual(s) shall be made in writing and delivered by first-class mail to the individual at the last known address of the individual, as indicated in the clinical data repository (CDR) maintained by GNOHIE.
- ii. Notification may be provided in one or more mailings, without unreasonable delay, as information is available.
- iii. If GNOHIE's CDR indicates that the individual is deceased and the address of the next of kin or personal representative of the individual is available in the CDR, written notification by first-class mail may be provided to either the next of kin or personal representative of the individual.

6. Substitute Notice. In the case in which Participating Organization, Member, or PATH is required to provide notice to affected individuals and GNOHIE's CDR has insufficient or out-of-date contact information that precludes written notification to the individual, Participating Organization or Member or PATH may use a substitute form of notice reasonably calculated to reach the individual.

- i. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.
- ii. If GNOHIE has insufficient or out-of-date contact information for fewer than 10 individuals, Participating Organization, Member, or PATH can provide notice by telephone, or other means. iii. If GNOHIE has insufficient or out-of-date contact information for 10 or more individuals, Participating Organization, Member, or PATH shall provide substitute notice:
 - a. Through a conspicuous posting for a period of 90 days on GNOHIE's website or in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
 - b. Include a phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may be included in the breach.

7. Urgent Situations. If PATH deems that a situation requires urgency because of possible imminent misuse of unsecured PHI, PATH may provide information to affected Participating Organizations and Members and/or individuals by telephone or other means, as appropriate, in addition to written notice.

C. NOTIFICATION TO MEDIA

- 1. Large-scale Breach.** If a breach involves more than 500 patients, PATH shall, on behalf of the affected Participating Organizations or Members, notify prominent media outlets serving New Orleans without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
- 2. Contents of Notification.** Notification to the media must contain the same information as notification to affected individuals. The Notification shall not contain any PHI. PATH will work with all affected Participating Organizations on the content and timing of the notification.

D. NOTIFICATION TO SECRETARY

- 1. Immediate Notification for Large-Scale Breach.** For breaches involving 500 or more individuals, PATH shall, on behalf of the affected Participating Organizations or Members, notify the Secretary of Health and Human Services through HHS website within 60 calendar days from the discovery of the breach:
https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true
- 2. Annual Notification for all Breaches.** For breaches involving fewer than 500 individuals, PATH will notify the Secretary of the breach within 60 days of the

end of the calendar year in which the breach was discovered. (A covered entity or their business associate is not required to wait until the end of the calendar year to report breaches affecting fewer than 500 individuals; a covered entity or their business associate may report such breaches at the time they are discovered.) The covered entity or their business associate may report all of its breaches affecting fewer than 500 individuals on one date, but the covered entity or their business associate must complete a separate notice for each breach incident. The covered entity or their business associate must submit the notice electronically by clicking on the link below and completing all of the fields of the breach notification form.

https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

Associated Policies:

1. Patient Consent
2. Data Use, Retention and Disclosure
3. User Access Control