PATHWAYS CMH

PROCEDURE TITLE: Pathways Breach Notification Procedure – Appendix 18 of Privacy Policies	**CATEGORY:** Recipient Rights
EFFECTIVE DATE: August 2010	**BOARD APPROVAL DATE:** August 2010
REVIEWED DATE: June 2013; July 11, 2014; May 5, 2015; April 28, 2016; April 15, 2017	**REVISION(S) TO PROCEDURE:** ☐ **Yes** ☒ **No**
RESPONSIBLE PARTY/APPROVAL: Recipient Rights Supervisor or Designee/ Mary J. Swift, CEO	

PURPOSE:

To ensure compliance with regulatory standards regarding breaches of privacy and breach notification requirements.

DEFINITIONS

1. ***Breach:*** Means an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information.
There are three exceptions to the definition of "breach" which are:

i. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of Pathways or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted.

ii. Any inadvertent disclosure by an employee who is authorized to access protected health information to a business associate or another employee authorized to access protected health information and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted.

iii. A disclosure of protected health information where Pathways or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2. ***Unsecured protected health information***: means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section13402(h)(2) of Public Law 111–5 (HITECH Act) on the HHS Web site.

3. ***Workforce:*** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Pathways or a business associate, is under the direct control of Pathways CMH or a business associate, whether or not they are paid by Pathways or a business associate.

PROCEDURES:

I. Administrative Requirements and Burden of Proof

A. An impermissible use or disclosure of protected health information (PHI) is presumed to be a breach unless Pathways or its business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:
   1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   2. The unauthorized person who used the PHI or to whom the disclosure was made;
   3. Whether the PHI was actually acquired or viewed; and
   4. The extent to which the risk to the PHI has been mitigated.

B. Policies, Training, and Enforcement
Pathways will have in place written policies and procedures regarding privacy of PHI and breach notification.

C. Training:
All members of Pathways workforce will be trained on the policies and procedures with respect to protected health information required by this procedure as well as Pathways Privacy and Security practices, as necessary and appropriate for the members of the workforce to carry out their functions.

D. Refraining From Intimidating or Retaliatory Acts
Pathways may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this procedure or any Privacy Practices, including the filing of a complaint under this section;

E. Waiver of Rights
Pathways will not require individuals to waive their rights under federal privacy laws as a condition of the provision of treatment, payment, enrollment or eligibility for benefits.

F. Sanctions:
See Pathways Privacy Practices, Appendix #17.

II. Reporting Requirements

Any workforce member who believes there has been a breach of protected health information shall notify their supervisor and Pathways Security Officer immediately.

Pathways Security Officer will notify the Pathways Security Incident Response Team (SIRT) to immediately determine whether a breach has occurred. This analysis will include determination of whether there was a violation of the Privacy Rule and whether the violation compromises the security or privacy of the protected health information. Pathways will maintain documentation of this analysis.

Pathways will ensure all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach. With respect to an impermissible use or disclosure, Pathways will maintain documentation that all required notifications were made, or alternatively, documentation to demonstrate that notification was not required, such as: (1) the risk assessment demonstrating a low probability that

the PHI has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of "breach."

III. Breach Notification Requirements

A breach shall be treated as discovered as of the first day on which such breach is known by Pathways, or by exercising reasonable diligence would have been known to Pathways. Pathways shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent.

Following the discovery of a breach of unsecured protected health information, Pathways shall notify each individual whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach.

A. Individual Notice

Pathways shall notify affected individuals in written form by first class mail to their last known address. Notice must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The notification may be provided in one or more mailings as information is available. If the individual is deceased written notification by first class mail will be sent to the personal representative of the individual, if known.

The Notice shall include:

1. A brief description, in plain language, of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. A description of the types of unsecured protected health information 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);

3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

4. A brief description of what Pathways is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

5. Contact procedures for individuals to ask questions or learn additional information, which shall include Pathways a toll free telephone number and e-mail address.

If Pathways knows the individual is deceased and has the address of the personal representative of the individual, written notification by first class mail will be sent to the personal representative of the individual.

B. Substitute Notice- Insufficient or Out-of-Date Contact Information:

If Pathways has insufficient or out-of-date contact information for **fewer than 10** individuals, Pathways may provide substitute notice by an alternative form of written notice, by telephone, or other means. 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 personal representative of the individual.

If Pathways has insufficient or out-of-date information for **10 or more** individuals, Pathways must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast medical where the affected individual likely reside. A toll-free phone number that remains active for at least 90 days must be included.

These notices must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, the same information included in an Individual Notice.

C. Additional Notice in Urgent Situations:
If Pathways deems a breach to be a potential for imminent misuse of unsecured PHI, Pathways may provide information to individuals by telephone or other means, as appropriate, in addition to the written notice.

D. Notification to the Media:
For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, Pathways shall notify prominent media outlets serving the State or jurisdiction. Media notification shall be provided without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. Media notification shall include the same information required for the individual notice.

E. Notification to the Secretary of Health and Human Services:
In addition to notifying affected individuals and the media (where appropriate), Pathways must notify the Secretary of breaches of unsecured PHI. Notification is made electronically at the HHS web site on the breach report form provided. If a breach affects 500 or more individuals, Pathways must notify the Secretary without reasonable delay and in no case later than 60 days following the discovery of a breach. If however, a breach affects fewer than 500 individuals, Pathways may notify the Secretary of such breaches on an annual basis, no later than 60 days after the end of the calendar year in which the breaches are discovered.

F. Notification to a Covered Entity
If Pathways is a business associate of another covered entity, Pathways will notify the covered entity immediately following the discovery of a potential breach of the covered entity's protected health information. The covered entity will file necessary notification to individuals, Secretary of HHS and the media, as applicable, unless stated otherwise in the Business Associate Agreement.

G. Notification by a Business Associate:
A business associate shall notify Pathways immediately following the discovery of a breach of unsecured protected health information as outlined in this policy. Pathways, as the covered entity, is responsible for breach notification to the individual, Secretary of Health and Human Services, and the media, as required, unless delegated to the Business Associate and stated in the Business Associate Agreement.

A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall

be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

The notification required by a business associate shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

A business associate shall provide Pathways with any other available information that the Pathways is required to include in notification to the individual at the time of notification or promptly thereafter as information becomes available.

H. Law Enforcement Delay:
If a law enforcement official states that a notification, notice, or posting required under this procedure would impede a criminal investigation or cause damage to national security, Pathways or a business associate shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (A) of this section is submitted during that time.

IV. When is Breach Notification Not Required?

Required notifications are only required if the breach involved unsecured protected health information. Encryption and destruction are technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. Covered entities and business associates that secure information as specified by this guidance are not required to provide notifications following the breach of such information.

REFERENCES:

45 CFR § 164 Privacy of Individually Identifiable Health Information
45 CFR § 164.400-414 Breach Notification Rule
Public Law 111-5 Health Information Technology for Economic and Clinical Health Act (HITECH Act)