| | PCHP.PV.134 Breach Notification V4<br>PCHP.PV.134 | |
|---|---|---|
| CENTRA | Name: | PCHP.PV.134 Breach Notification |
| | ID Number: | PCHP.PV.134 |
| | Approval Date: | 02/04/2019 |
| | Approved By: | Garland Morton |

## Body

**Policy Name:** Breach Notification

**Scope:** Entire Piedmont workforce

**Purpose:** To ensure proper identification and timely notification to the proper individuals regarding a breach of PHI in accordance the HIPAA Final Rule.

**Definitions & Acronyms:**

CMS: Centers for Medicare & Medicaid
CFR: Code of Federal Regulations
PBM: Pharmacy Benefit Manager
HIPAA: Health Insurance Portability and Accountability Act of 1996
HITECH: Health Information Technology for Economic and Clinical Health Act
PHI: Protected Health Information
PII: Personally Identifiable Information
DRS: Designated Record Set
BA: Business Associate

**Piedmont:** "Piedmont" collectively refers to Piedmont Community Health Plan (PCHP), Piedmont Community HealthCare (PCHC) and any future entities that are owned, affiliated with and/or operated by Piedmont.

**Breach:** the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of 45 CFR 164 which compromises the security or privacy of the PHI.

1. Breach excludes:

   - Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or BA, 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 under subpart E of 45 CFR 164.
   - Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or BA to another person authorized to access PHI at the same covered entity or BA, or organized health care arrangement in which the covered entity or BA participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted un subpart E of 45 CFR 164.
   - A disclosure of PHI where a covered entity or BA 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. A breach is presumed unless the covered entity or BA demonstrates that there is a low probability that the PHI has been compromised based on a ***risk assessment*** of at least the following factors:

   - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   - The unauthorized person who used the PHI or to whom the disclosure was made;
   - Whether the PHI was actually acquired or viewed; and
   - The extent to which the risk to the PHI has been mitigated.

**Policy:**

1. Piedmont will investigate all incidents reported by individuals, employees, and business associates, and provide timely notification as necessary and appropriate to:
    a. Affected individuals,
    b. Media outlets,
    c. The Secretary (Department of Health and Human Services),
    d. Credit reporting agencies,
    e. Other federal or state agencies,
    f. Law enforcement, if necessary, and
    g. CMS, if applicable.

2. Piedmont will provide training to all workforce employees on the Breach Notification Rule.

3. Piedmont will provide a process for individuals to complain about Piedmont's compliance with the Breach Notification Rule. Employees will not retaliate against employees and individuals who submit complaints and notifications of potential violations of the Breach Notification Rule in good faith.

4. Piedmont will provide appropriate sanctions to individuals who are found to have violated the Breach Notification Rule.

5. Piedmont prohibits the practice of requiring a waiver of rights to Breach Notification by members as a condition of receiving treatment, payment or enrollment in the health plan and eligibility of its benefits.

6. Piedmont will perform a breach risk assessment for each reported incident of potential HIPAA breach violation. The following circumstances apply to all potential HIPAA Breaches:
    a. Any incident is presumed to be a Breach and notification is necessary unless a low probability exists that PHI has been compromised.
    b. If the risk assessment determines that a reportable breach has occurred, Piedmont will timely notify all affected members that are subject to the breach.
    c. If over 500 individuals' PHI was breached, Piedmont will notify prominent media outlets no later than 60 calendar days after discovery of a breach

7. Piedmont will accommodate requests by law enforcement to delay notification to a member under the Breach Notification Rule under certain circumstances.
8. Piedmont has the burden to prove and demonstrate that all notifications were made with appropriate content and timeliness as required.
9. The Compliance Officer will maintain documentation related to all incidents, including the risk assessment and all notices for a period of at least 6 years.

**Procedures:**

1. Piedmont employees will immediately report known or suspected incidents of breach to his/her Manager or Director, who will report the breach to the Compliance Officer or Department.
2. The Compliance Officer, or his/her designee, will investigate the reported HIPAA incident by emailing or calling the Piedmont employee(s) that was involved in the disclosure of PHI within a reasonable amount of time of the incident. Additional investigation through review of calls, emails, evidence of PHI should occur within 14 days of the identification of the issue.
3. The Compliance Officer, or his/her designee, in conjunction with the IT department, legal counsel and/or others as appropriate, will take immediate steps to investigate and contain the incident and mitigate risk of harm to affected individuals.
4. In the event the incident involves possible criminal activity, such as identity theft or theft of valuable Piedmont equipment or proprietary information, the Compliance Officer will file a police report or other notification with the appropriate law enforcement division.
5. All Piedmont staff will be trained on how to recognize and report incidents of breach. Training could include departmental classroom-style trainings, and Computer-Based Learning (CBL) modules, one-on-one training, etc.
6. Complaints: See PCHP.CP.104 Effective Communication for Piedmont's policy on communication and confidential methods of reporting non-compliance.

7. Sanctions: Piedmont will provide consistent sanctions to those employees found to have violated the Breach Notification Rule in timeliness, content, risk assessment, etc., which could include the following:

   A. Verbal warning

   B. Written warning

   C. Documentation in the employee's personnel file

   D. Multiple offenses could be up to and including termination.

8. The Compliance Officer, or his/her designee, will perform a risk assessment to determine whether the incident qualifies as a Breach under applicable federal and/or state notification laws.

   A. The risk assessment is performed to determine if low probability exists that PHI has been compromised, and includes the following:

      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. Breach Risk Assessments should be performed within 30 days of identification of the issue to allow ample response time to prepare any necessary notification letters.

9. Upon determination of a Breach, the Compliance Officer, or his/her designee, will take all reasonable measures to notify affected individuals.

   A. The notification must include:

      1). Brief description of what happened, including the date of breach and date of discovery,

      2). Types of unsecured PHI that was involved in the breach (i.e. whether full name, SSN, date of birth, account number, diagnosis, or other types of information involved),

      3). Steps individuals should take to protect themselves from potential harm resulting from the breach,

      4). Brief description of what Piedmont is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches,

      5). Contact information for questions.

   B. The notice must be provided without unreasonable delay, and no later than 60 days after discovery of breach.

   C. Methods of notification include:

      1). Written notification by mail (or electronic mail if requested by member). In the event member is deceased, next of kin or personal representative will be notified, if known.

      2). In the event there is insufficient or out-of-date contact information for individuals, a substitute form of notice must be used.

         i. In cases involving less than 10 individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means.

         ii. In cases involving more than 10 individuals, the substitute notice must:

            (a) Be in the form of either a conspicuous posting for a period of 90 days on the home page of Piedmont's website, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected likely reside.

            (b) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether their unsecured PHI may be included in the breach.

      3). In urgent situations, Piedmont may provide information to individuals by telephone or other means, in addition to notice requirements above.

10. The Compliance Officer will notify federal and state agencies, media outlets, credit reporting agencies and other individuals as necessary and appropriate. All notifications will be made in accordance with regulatory requirements and without reasonable delay (subpart D of 45 CFR 164).

    A. Prominent media outlets will be notified no later than 60 calendar days after discovery of a breach for a

breach of unsecured PHI involving more than 500 members.

B. HHS will be notified in the manner specified on the HHS Web site for breaches involving 500 or more individuals.

C. For breaches involving less than 500 individuals, Piedmont will maintain a log (Breach Notification Log located at S:\HIPAA\Disclosure Logs) or other documentation of such breaches, and notify the HHS in the manner specified on the HHS Web site no later than 60 days after the end of each calendar year.

D. Piedmont will report any Breach of PII related to the Exchange product to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within 24 hours from knowledge of the Breach. Incidents will be reported to the CMS IT Service Desk by the same means as Breaches within 72 hours from knowledge of the Incident.

11. The Compliance Officer may take additional actions as necessary and appropriate to safeguard PHI and PII and to mitigate harm. This includes, but is not limited to:

A. Providing identity theft protection services to affected individuals,

B. Re-training and educating staff members,

C. Implementing or recommending the implementation of controls to prevent further breaches, and

D. Recommending disciplinary action up to and including termination.

12. Business Associates must follow the same breach requirements and must notify Piedmont of such breach.

**Equipment:** None

**Forms and Letters:** None

**Reference(s):** 45 CFR §164 Subpart D – Notification in the Case of Breach of Unsecured Protected Health Information; 45 CFR §164.530 b, d, e, g, h, i, and j

**Interdisciplinary Review:** None

**Policy History:**

| Date | Revision No. | Reason for Change | Sections Affected |
|---|---|---|---|
| 09/23/2013 | NEW | | All |
| 02/02/2016 | 1.1 | Converted to Centra Format | |
| 07/18/2016 | 2.0 | • Reviewed for compliance with Phase 2 Audit Protocol<br>• Reviewed for compliance with NCQA Standards 2016<br>• Incorporated new policy language, moved other procedural language into the policy. | |
| 2/10/2017 | 3.0 | • Updated as a result of the issue ticket ML006 | Procedure 2; Procedure 8B |
| 2/4/2019 | 4.0 | • Updated to include CMS reporting requirements for CMS<br>• Clarified Policy 6c | Policy 1g; Procedure 10D |

**Document Link Manager**

**No Documents Linked** **No Documents Linked**

## Attachment Manager

**No Attachments**