| Heritage Provider Network & Affiliated Medical Groups | Program: HIPAA Compliance | | |
|---|---|---|---|
| | Policy No. | Effective Date: 01/01/2012 | Page - 1 - |
| | Authored by: Compliance Sub Committee / Date: 01/01/2012 | Revised by: Sandy Finley / Date: 09/16/2015 | |
| | Approved by: Compliance Sub Committee / Date: 09/23/2015 | | |
| Title of Policy: Notification and Investigation of Breach | | | |

PURPOSE:

To ensure that employees of Heritage Provider Network and its Affiliated Medical Groups (HPN) are familiar with the proper methods for notification of a possible breach and to ensure that all incidents are reported timely in order to conduct an investigation and minimize risk.

POLICY:

Employees and FDRs of HPN are required to report any identifiable issue or concern regarding possible violations to the group Compliance Officer. The group Compliance Officer will review issues/concerns for potential violations, conduct a timely investigation and implement appropriate corrective actions with the guidance from the Director of Human Resources.

DEFINITION:

Breach – an impermissible use or disclosure under the HIPAA/HITECH Act that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

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

RESPONSIBILITY:

All employees and FDRs of Heritage Provider Network and its Affiliated Medical Groups, Compliance/Privacy Officer and Human Resources.

PROCEDURES:

1. HPN employees and FDRs are to promptly report any suspected or potential non-compliance incidents by filing a report with their supervisor or to their Compliance Officer, or by calling the confidential Hotline at (855) 682-4127.

2. Reported issues and/or concerns are reviewed by HPN's Affiliated Medical Group Compliance Officer or designee. The Compliance Officer or designee utilizes Heritage Provider Network's compliance tools, such as the Risk Assessment, to determine whether the breach has a low or high breach risk. Assessment of the risk level is conducted without delay and is recorded and maintained by each HPN group's Compliance Officer. Investigations are initiated as quickly as possible, but no later than 10 days after the potential breach, noncompliance, or FWA is identified.

   The Risk Assessment of the alleged breach is to include:
   a. Whether or not there has been impermissible use, acquisition, access or disclosure of PHI in a manner not permitted under the HIPAA/HITECH Act.
   b. Whether or not the incident falls under one of the breach exceptions.
   c. The level of probability that the PHI has been compromised based on:
      i. The nature and extent of PHI involved
      ii. The unauthorized person who used the PHI or to whom the disclosure was made.
      iii. Whether the PHI was actually acquired or viewed
      iv. The extent to which the risk has been mitigated.

3. Results of investigations are referred to the appropriate department manager for review; and with guidance from the Human Resources Director an appropriate corrective action plan is implemented.

4. If a breach is established, immediate steps to reduce or eliminate any harmful effects of the breach will be taken. Notification of unsecured patient information will be reported to the appropriate entities in accordance with the Health Information Technology for Clinical and Economic Health (HITECH) Act.

5. All breaches of unsecured PHI, regardless of the number of patients affected will be recorded and logged on the Incident Notification Log form. The information must include, to the extent possible:
   a. The incident number;
   b. Company name/ID and location where the breach occurred;
   c. Contact information of Compliance Officer or of the entity that caused the breach;
   d. The date of discovery and the date of the breach occurrence;
   e. A brief description of the breach, including circumstance and personal information of any and all individuals of whose PHI was involved in the breach (e.g. full name);
   f. Type of breach;
   g. Reporting method;
   h. Number of individuals involved/affected by breach;
   i. Indication of HMO or ACO patient;

j. Notification dates to the patients, media, and HHS, as applicable;
k. Steps affected individuals should take to protect themselves from potential harm;
l. Actions taken for resolution, including steps for investigation, mitigation of losses (e.g. possible credit monitoring if breach included SSN, full name and date of birth), and actions to safeguard against future breaches.

6. A frequent analysis of the Incident Notification Logs will be conducted by HPN Affiliated Medical Groups' Compliance Officers to determine what types of breaches are occurring. Based on this analysis, further corrective action plans will be implemented (e.g. additional training and education, disciplinary actions).

7. Breach notifications will be provided to all affected members without unreasonable delay, but no later than 60 days from the day of discovery. All identified breaches will be reported to the appropriate government agency as required:
    a. For breaches affecting fewer than 500 individuals, a report will be submitted to the HHS annually within 60 days of the end of the calendar year in which the breaches occurred.
    b. For breaches affecting 500 or more individuals, a report will be submitted to the HHS and to the media without unreasonable delay, but no later than 60 days from the discovery of the breach.

8. Discovery and investigations of breaches are reported promptly, or as required by the health plans, providing to the extent possible the information indicated in section 5a-l.

REFERENCES:

45 CFR § 164.400-414