Privacy Breach Response Plan

Effective Date: 7/28/2014 Draft/Review Date: 8/18/2014

Policy

A. It is the policy of the ACO to respond to any potential privacy breach quickly and effectively, and, to the extent practicable, minimize any harmful effect that is known to the ACO of a use or a disclosure of Protected Health Information (PHI) in violation of the ACO's HIPAA Privacy policies and procedures or the requirements of 42 C.F.R. Part 164, Subpart E by either the ACO, its Participants, Providers/Suppliers, or any other individuals or entities performing functions or services related to the ACO's activities (hereinafter referred to as "Business Associates").

Applicability

This policy and procedure applies to all Participants, Providers/Suppliers, and other individuals or entities performing functions or services related to the ACO's activities.

Procedure

A. Information regarding any suspected or expected breach of PHI by the ACO or any of its Business Associates discovered by any individual or entity shall be forwarded promptly to the Compliance Officer.

    1. An entry will be created in the Privacy Incident Log.

B. The Compliance Officer will contact all individuals of the ACO who are relevant to the report.

    1. The contacted group, in response to such reports, including self-disclosures made by the Business Associates pursuant to the terms of each Business Associate's contract or other agreement with the ACO, shall develop and implement a plan as soon as reasonably practicable to mitigate any known or reasonably anticipated harmful effects of such act.

        a. Examples of immediate actions which may need to be considered are:

            i. Shutting down accesses or systems which may be vulnerable.

            ii. Shutting down public access to web pages where information is found.

            iii. Contacting the recipient of the information that was disclosed and instructing such recipient to either destroy or return the information and to make no further use or disclosure of such information.

    2. If necessary, the Compliance Officer will contact designated outside Counsel to help analyze the situation.

    3. Once the incident has been contained, the contacted group will discuss and perform a risk assessment to determine whether or not a Reportable Breach has occurred. This assessment will include:

        a. Whether there has been impermissible access, use or disclosure of PHI;

b. Who impermissibly accessed, used or received PHI and to whom the PHI was potentially disclosed, if applicable;

c. Whether the PHI involved in the incident was Unsecured PHI;

d. The type and amount of PHI involved; and,

e. What steps have been taken (or should be taken) to mitigate risk.

C. If it is determined that a Reportable Breach has occurred, the Compliance Officer may determine it is necessary to contact designated outside Counsel. This Information can be found on the Breach Response Contact Sheet.

1. The breach should be reported to appropriate State and Federal entities, as required.

a. Reporting to the Office of Civil Rights:

i. If less than 500 individuals are impacted, the disclosure shall be logged with the OCR at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html not later than 60 days after the end of the calendar year.

ii. If more than 500 individuals are impacted, the disclosure must be logged with the OCR at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html within 60 days of the discovery and a press release issued to the media in the state impacted.

b. Reporting to CMS

i. The update to the Medicare Regional Office Account Manager will include:

a) If the Office of Civil Rights was notified, a copy of the breach report provided to the Office of Civil Rights.

b) If the Office of Civil Rights was not notified yet, the notice to the Medicare Regional Office Account Manager should include an account of the breach with as much information as possible.

c) The number of Beneficiaries impacted.

d) Any actions being taken to mitigate the risk to the Beneficiaries.

D. The Compliance Officer, in conjunction with the other relevant business areas, will determine what steps are required to mitigate the situation, including offering credit monitoring for affected individuals.

E. The Compliance Officer will prepare a Notice Letter to Beneficiaries, as required. A model Notification Letter is attached to this policy.

1. Individual Notifications will be made without unreasonable delay, but in no event more than 60 days from the date of discovery of the Reportable Breach. The ACO may delay notifications if a delay is requested by a law enforcement official.
2. Notice must be provided through a press release to prominent media in the state of the disclosure if more than 500 individuals of a state are impacted.
3. Notifications will be written in plain language, at an appropriate reading level, and must include the following information:
    i. A brief description of what happened, including the date of the Reportable Breach and the date of discovery of the breach, if known;
    ii. A description of the types of Unsecured PHI that were involved in the Reportable Breach;
    iii. Any steps individuals should take to protect themselves from potential harm resulting from the Reportable Breach;
    iv. A brief description of the ACO's efforts to investigate the breach, mitigate harm to individuals, and protect against further Reportable Breaches; and,
    v. Contact information for individuals to ask questions or learn information about the Reportable Breach, which must include a toll-free telephone number, an email address, website, or postal address.

F. The Compliance Officer will follow up to determine whether changes to the ACOs Privacy Policies, disciplinary action, or additional training are necessary to prevent further incidents.

Reporting

A. Reporting may be required under State and Federal Laws.

Related Documentation

A. ACO Terms & Definitions Policy

B. Model Notification Letter