Policy Number: HC-27	Page: 1	Of: 3
Title: Breach Reporting		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

(A) Breach Reporting
The board will notify Individuals receiving services, the Secretary of HHS and, when appropriate, the news media regarding breaches of protected health information.

Audience

Hipaa security officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164, Subpart D

164.400, 164.402, 164.404, 164.406, 164.408, 164.410, 164.412, 164.414

1) Upon becoming aware of a privacy rule violation or security incident, the HIPAA Privacy Officer and the Superintendent shall jointly determine if the incident meets the definition of a breach. If a Security Incident Response Team (Team) has not been assembled, they may assemble a Team at this point. Legal counsel and other outside expert advice shall be obtained, if appropriate, for additional guidance on the Team. An investigation should be launched, with attention to preserving evidence. The Team shall follow the following 3 step procedure:
   a) Was there acquisition, access, use, or disclosure of PHI that violates the Privacy rule? If "no", there is no breach. Otherwise, proceed to the next step.
   b) Does one of the statutory exceptions listed in the breach definition in Policy apply? If "yes", there is no breach. Otherwise, proceed to the next step.
   c) Unless the incident is clearly a breach, the Team shall conduct a risk assessment. The risk assessment, per HIPAA regulations, shall consider at least the following factors:
      i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
      ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
      iii) Whether the protected health information was actually acquired or viewed; and
      iv) The extent to which the risk to the protected health information has been mitigated.

The results of this evaluation shall be documented and maintained for 6 years as detailed in Policy 1330 HIPAA Assignments and Documentation. If the risk assessment demonstrates

that there is a low probability that PHI has been compromised, then no breach has occurred and this process may stop. Otherwise, a breach has occurred and the Team should proceed with the steps that follow in the remainder of this policy.

2) **Public Relations Strategy**. The Team should develop a public relations strategy to include when and who should speak to the media and what should be said.
3) **Breach Notification**. In the event of a breach, the Team shall:
   a) Notify Individuals affected by the breach without unreasonable delay (and in no case later than 60 calendar days after the discovery of the breach):
      i) In the event of an urgent situation, the board may use telephone, email or other means to immediately notify individuals of the breach.
      ii) Prepare formal written notification for approval by superintendent. The notification shall be written in plain language and include the following:
         1) A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;
         2) A description of the types of unsecured protected health information that were involved in the breach;
         3) Any steps that individuals should take to protect themselves from potential harm resulting from the breach;
         4) A brief description of what the board 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 a toll-free telephone number, an e-mail address, web site or postal address.
      iii) Send the primary breach notification to:
         1) Individuals affected by the breach by first-class mail at their last known address, or by e-mail if agreed in advance by the individual for this type of notice, or
         2) Parent, guardian, or HIPAA Personal Representative of the Individual in the event the individual is a minor and/or not competent to make decisions, or
         3) next of kin or personal representative of the Individual in the event that the individual is deceased and the next of kin name and address are available.
      iv) Track returned mail and provide a substitute notice to Individuals who did not receive the primary notification (no further effort is necessary for unreachable next-of kin):
         1) In the event that fewer than 10 individuals, the HIPAA Security Officer shall research updated address and/or phone number and make best efforts to inform those individuals by either phone or mail.
         2) In the event that 10 or more individuals are not reachable by first class mail,
            a) A toll-free phone number shall be established, and staffed with operators, for at least 90 days
            (a) a notice shall be conspicuously placed on the board's web site home page with details of the above details on the breach plus the phone number
   b) Notify the news media if more 500 Individual records are involved in the breach

i) Under direction of the board superintendent, a press release shall be prepared detailing the information in section 2Ab above, and other relevant information.
ii) Upon approval of the board superintendent, the press release shall be issued without unreasonable delay (and in no case later than 60 days after discovery of the breach) to the major print, broadcast and online media serving the county.

c) Notify the Secretary of the Department of HHS regarding the breach
i) In the event that the breach involves 500 or more individuals, notice to the Secretary should be provided at the same time as the Individual notification in the manner detailed on the HHS Web site.
ii) For breaches involving fewer than 500 individuals, a log including at a minimum the information in 2Ab above, and other relevant information, should be maintained. At the end of the calendar year, the contents of the annual log should be provided to the secretary in the manner detailed on the HHS Web site.

2) **Breaches by Business Associates**. Breaches by business associates are handled in the same manner. Business associates are obligated to cooperate in providing necessary information; the board is responsible for issuing the notice detailed in this policy.

3) **Law Enforcement Delay**. The notices to Individuals and the media may be delayed if a request is received by a law enforcement official:
a) If written notice is received from a law enforcement official which specifies the time period of delay, the board shall comply with that request.
b) If the request is made orally, the notification shall be delayed but not longer than 30 days from the date of the oral request.

4) **Documentation**. Documentation, including any notices provided, incident reports, meeting notes, especially those which document the date of the breach, shall be maintained for 6 years. For the legal purposes, including the timelines in policy, the date of breach discovery shall be the date that the board should have become aware if it exercised reasonable diligence.