BREACH OF PERSONAL CLIENT INFORMATION

Section: HIPAA

Pages: 2

Subject: Breach of Personal Client Information

Effective Date: 09/2017

Revision Date: 03/03/2020

POLICY

Davis Behavioral Health will ensure protected health information is free from unauthorized use or disclosure. In the event of a breach of such protections, DBH shall immediately take appropriate steps of mitigation. DBH will report any breach in compliance with federal privacy regulations.

PROCEDURE

1) DEFINITIONS
   a) A breach is defined as an unauthorized access, acquisition, use or disclosure that compromises the security or privacy of protected health information ("PHI"). A breach may include but is not limited to discussing PHI in public places, leaving documents containing PHI in public places, posting PHI on unsecured websites, sending PHI in email outside the DBH system, and misplacing or losing unencrypted PHI stored on removable computer media.

2) A breach does not include:
   a) Any unintentional acquisition, access, use or disclosure of PHI by an employee or other individual acting under the authority of DBH or its business associate if:
      (1) Such acquisition, access or use was made in good faith and within the scope of authority; and
      (2) Such information is not further acquired, accessed, used or disclosed in a manner not permitted by privacy regulations
   b) Any inadvertent disclosure of PHI from an authorized individual within DBH (or its business associate) to another similarly situated individual at the same facility, and
      (1) Such further information is not further acquired, accessed, used or disclosed in a manner not permitted by privacy regulations.
   c) Any disclosure where DBH has a good faith belief that the unauthorized person to whom the disclosure was made would not have been able to retain the information.

3) MITIGATION
   a) Any DBH staff member who observes a potential breach shall immediately take steps to mitigate the unauthorized use or disclosure, when possible. Appropriate steps are specific to each situation and may include, but are not limited to, one or more of the following:
      (1) Interrupting or terminating a verbal discussion in a public area accessible to unauthorized individuals;

(2) Retrieving and properly storing or disposing of a document containing PHI which has been left in a public area;
(3) Securing and locking an area which provides access to PHI;
(4) Making effort to retrieve a misplaced or lost item or record containing PHI;
(5) Securing an affected computer system and restoring PHI;
(6) Retrieving mail that was sent to the incorrect address or receiving assurance from the recipient that it was properly destroyed

4) DOCUMENTATION

a) Any breach, whether intentional or unintentional, as defined in Section I above shall be immediately reported to the Privacy Officer. An intentional breach may also result in further disciplinary action, up to and including termination of employment.

b) Upon receiving notification of an alleged breach, the Privacy Officer shall coordinate an investigation and ensure complete documentation on the Privacy Incident Tracking Report. The report shall include, at minimum, the following information of the incident:
(1) Date, time and location
(2) Specific description of allegation, including any harm known or observed
(3) Type and formal of PHI disclosed (paper records, electronic records, verbal disclosure, other)
(4) List of other persons involved, including name(s), title(s), and contact information
(5) Steps of mitigation immediately taken, if any

5) Any unauthorized access, acquisition, use or disclosure of PHI is presumed to be a breach unless the Privacy Officer determines there is a low probability the PHI has been compromised. This determination is based upon a risk assessment of at least the following factors:

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

6) CORRECTIVE ACTION AND NOTIFICATION

a) Upon completion of the risk assessment, if the Privacy Officer determines that there is a reasonable belief that an individual's PHI was accessed, acquired, used or disclosed by an unauthorized individual, the Privacy Officer shall immediately coordinate a corrective action plan with the supervisor of the program staff responsible for the breach. Further disciplinary matters, if applicable, will be referred to Human Resources.

b) The Privacy Officer will make reasonable efforts to notify any affected individuals or other interested parties in compliance with the standards listed below:
(1) Notification of Individuals – 45CFR 164.404
(2) Notification to the Media – 45 CFR 164.406
(3) Notification to the Secretary – 45 CFR 164.408

Reference: HIPAA Breach Notification Rule, 45 CFR 164.400 – 414.