

Advanced Heart and Vascular Center			
Policies and Procedures			
Policy Code: IM.002		Breach Notification of Protected Health Information	
Approved By: Sandra Germany, Administrator	Effective Date: 06/18	Review Date: 5/26	Revision Date:

PURPOSE

To provide Advanced Heart and Vascular Center (“AHVC”) employees, healthcare workers, and associates with guidelines and processes for breach notifications when unauthorized access, acquisition, use, and/or disclosure of AHVC patient PHI occurs.

POLICY

AHVC will follow Protected Health Information (“PHI”) breach notification procedures in accordance with federal or state notification laws.

- AHVC will provide education on how to identify and report PHI breaches. Some examples of PHI breaches include:
 - Accessing a friend's medical record
 - Lost or stolen laptop with PHI
 - Theft of a car with a briefcase containing medical records
 - Fax with PHI sent to the wrong location
 - Medical records sent to an insurance company but are lost in the mail
 - Patient care notes that have fallen out of someone's pocket
 - Posting any patient information or pictures on Facebook, Twitter, or the internet
 - Sending an unencrypted email containing patient information
- Breach notification applies to all unauthorized uses and/or disclosures of PHI, regardless of the number of patients involved.

PROCEDURE

- As soon as the breach is discovered, employees and associates will notify their supervisors or the Administrator. Employees and associates should provide as much detail as possible, including the identity of each individual whose PHI has been accessed, acquired, or disclosed.
- The Administrator will be immediately notified of all breaches.
- The Administrator or designee will conduct a review of the nature of the breach and determine if the breach was intentional/unintentional and the discipline policy to be followed.
- An intentional breach may receive at a minimum a written disciplinary warning and at a maximum, termination.
- An unintentional breach, with no intent to violate confidentiality or security will receive at a minimum education or training regarding confidentiality and/or security policies and procedures.
- Education starts at orientation with a confidentiality statement signed by all employees.

Should data or information confidentiality/security breaches occur by an individual not in the employment of AHVC, the following processes will be followed:

- Any staff member who obtains knowledge of a breach will report the incident to their supervisor or the Administrator.
- The Administrator will be immediately notified of all breaches.
- The Administrator or designee will determine the nature of the breach and results, including harm done by the incident.
- The Administrator will meet with appropriate AHVC staff to determine plans for future prevention and implementation of changes.
- AHVC will not, nor allow any of its employees to, intimidate, threaten, coerce, discriminate against, or take any other retaliatory action regardless of the outcomes of the review conducted by AHVC against:
 - Individuals who have reported violations of privacy or confidentiality;
 - Individuals who have filed a complaint with the Secretary of the Department of Health and Human Services or who have testified, assisted, or participated in an investigation, compliance review, proceeding or hearing; or

- Individuals who have opposed any act or practice that the individual in good practice believes violates the privacy regulations under HIPAA.

REFERENCES

45 CFR §§ 164.400-014