Policy 5
Security Incidents Policy and Procedure

Policy:

1. Identification and Reporting of Security Incidents

All employees will be responsible for identifying and reporting all security incidents of which they become aware.

A security incident shall have the same meaning as that set forth in the final HIPAA Security Rule, i.e., "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

Examples of security incidents that must be identified and reported, include, without limitation:

- Passwords that have been lost, stolen, shared, or used by persons other than the individual to whom the password was assigned
- Introduction of viruses, worms, Trojan horses or other malicious software into the organization's computer systems
- Unauthorized access to networks, computer systems, or facilities/equipment rooms housing the computer systems
- Destruction of electronic protected health information

2. Documentation of Security Incident and Response

When the Security Officer receives a report of a security incident, it will be the responsibility of the Security Officer to document the security incident, the outcome of the investigation and the organization's response to the security incident.

3. Mitigation of Harm

If a security incident results in an inappropriate disclosure of patient's protected health information, it will be the responsibility of the Security Officer to determine what steps can be taken to mitigate the harmful effects of any security incident. The steps taken should be documented.

4. Breach Notification

The Security Officer, in coordination with the Privacy Officer, will determine if any notifications must be made pursuant to the Breach Notification Rules.

Procedure:

1. Employees will be responsible for understanding the definition of a security incident and their responsibility for reporting such incidents to the Security Officer.
2. The Security Officer will be responsible for documenting all incidents, the results of the investigation, the response and steps taken to reduce harmful effects and maintaining such documentation for six (6) years.
3. The Security Officer will be responsible for determining what, if any, steps can be taken to mitigate the harmful effects of the breach. The Security Officer will also be responsible for taking such steps either personally or through delegation and documenting the steps taken. All documentation related to mitigation of harmful effects of a breach must be maintained for six (6) years.
4. The Security Officer will be responsible for coordinating with the Privacy Officer with regard to the appropriate notifications that must be made in order to comply with the Breach Notification Rule.

Explanation of the Security Incident Procedures Standard and Instructions for Utilizing the Security Incidents Policy

The Security Incident Procedures Standard requires covered entities to implement policies and procedures to address "Security Incidents." The standard contains one implementation specification - "Response and Reporting". This implementation specification requires organizations to identify and document all security incidents, the organization's response to the security incident, and the outcome of the response.

Policy 5 is a sample policy that could be used to address this standard and its implementation specifications.

A security incident is defined in the Final Rule as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

Examples of Security Incidents would be:

- Users attempting to login to the system multiple times with the wrong password
- Stolen passwords
- Password cracking (guessed passwords)
- Introduction of viruses or other malicious software into information systems
- Destruction or deletion of electronic protected health information
- "Hackers" or "Crackers" (unauthorized persons accessing networks or computer systems)

1. Response and reporting

a. General Requirements

The "Response and Reporting" implementation specification requires organizations to identify and document all security incidents, the organization's response to the security incident, and the outcome of the response.

b. Breach Notification

If a security incident results in a use or disclosure of protected health information that violates the HIPAA Privacy Rule, then the practice must consider whether reports must be made pursuant to the Breach Notification Rule.

An inappropriate disclosure of protected health information will only be considered a "breach" for purposes of the Breach Notification Rule if a determination is made that "there is a significant risk of financial, reputational or other harm to the individual." In making this determination, the following factors should be taken into account:

a. The identity of the entity or individual that impermissibly used the information or to whom the information was impermissibly disclosed;
b. The steps that were taken to mitigate harm and the immediacy with which such steps were taken;
c. Whether the information was returned before being accessed; and
d. The type and amount of information disclosed.

If the practice determines that the inappropriate use or disclosure of protected health information was a "breach" each affected individual must be contacted personally without unreasonable delay, but no later than 60 days after discovering the incident. The notice must be written in plain language and must include the following:

- A brief description of the incident, including the date of the breach and the date of discovery of the breach;
- A description of the types of unsecured information that were involved in the breach;
- Any steps that the affected individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the practice is doing to investigate the incident, mitigate harm to the affected individuals, and protect against further breaches; and
- Contact procedures for affected individuals to ask questions or learn additional information, including a toll-free telephone number, e-mail address, website or postal address.

The notification of breach must be sent via first class mail to the affected individual's last known address, unless the individual has agreed to receive notification electronically. If the affected individual is a minor or is incapacitated, notice of the breach must be provided to the individual's personal representative. If the affected individual is deceased, the practice must provide notice of the breach to the individual's next of kin or personal representative, if known.

The entity must also take any additional steps deemed necessary to mitigate harm to the individual.

In the event that the contact information for an affected individual or a group of affected individuals is insufficient or out-of-date so as to make the individual notice described above impossible, the practice must make substitute notice in accordance with the following procedures:

- If there are less than 10 affected individuals for whom there is insufficient or out-of-date contact information, substitute notice can be made to these individuals by telephone notice or by any other means.
- If there are more than 10 affected individuals for whom there is insufficient or out-of-date contact information, the practice must either post notice of the breach on its website homepage or publish notice in a print or broadcast medium that is a major media outlet for the geographical area. Such notice must remain posted for at least 90 days and must include a toll-free telephone number that individuals may call for information.

If a breach involves more than 500 individuals, the practice must publish notice of the breach in a prominent media outlet no less than 60 days after the discovery of the incident. The notice must include all of the information contained in an individual notice. Regardless of the number of individuals involved, all breaches must be aggregated and reported via the Office of Civil Rights website within 60 days after the end of the calendar year. Instructions and electronic forms are available at:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html