Greater Hudson Valley Health System
Policy/Procedure

MANUAL: Information Technology
SECTION: IT

SUBJECT: IT Security Incident Procedures #210010	
IMPLEMENTATION: 1/27/2005	CONCURRENCES: Compliance Department
REVIEWS: 2009	
REVISIONS: 2009, 2013, 4/14	
INITIATOR: HIPAA Security Officer	
APPROVAL: CIO	

Purpose:
The purpose of this policy is to establish guidelines for the identification, response, reporting, assessment, analysis, and follow-up to information security incidents. Greater Hudson Valley Health System (GHVHS) will create a processes for the identification, reporting, and ensuring a timely response to real or potential violations of the security or a material breach of any part of Greater Hudson Valley Health System's IT Security policy.

Scope:
This policy applies to GHVHS in its entirety, including all workforce members.
This policy applies to the following security incidents:

- Technical security incidents (e.g., computer intrusions, denial of service to authorized users, etc.)
- Non-technical security incidents (e.g., administrative and physical incidents including, but not limited to theft, unlocked doors, unauthorized facility entry, unauthorized computer access, etc.)

Policy:

- It is the Policy of GHVHS to rapidly identify and appropriately respond to all security incidents, regardless of their severity.
- Responsibility for responding to and managing security incidents shall reside with the Chief Information Security officer.
- It is the Policy of GHVHS to fully document all security incidents and our responses thereto.
- GHVHS staff are to report any and all possible breaches of Information Security or PHI upon observation. Refer to the HIPAA Breach & Discipline Policy for further information pertaining to HIPAA breach levels and disciplinary actions.

Key Definitions:
Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Indication: A sign that an incident may have occurred or may be occurring at the present time. Examples of indications include:

- The antivirus software alerts when it detects that a host is infected with a worm.
- The Web server crashes.

- The system administrator sees a filename with unusual characteristics.
- The user calls the help desk to report a threatening e-mail message (and it is determined by Information Services that it is a legitimate risk issue).
- Suspicious network and host-based IDS events/attacks.
- Alerts as a result of detecting malicious code at the network and host levels.
- Alerts from third party monitoring services.
- Audit log alerts.

Event: An event is defined as an occurrence that does not constitute a serious adverse effect on the organization or its operations, though it may be less than optimal. Examples of events include, but are not limited to:

- A hard drive malfunction that requires replacement
- Accidental lockout of an account due to incorrectly entering a password multiple times
- Network or system instability

Security Incident: A ***security incident*** is an occurrence that exercises a significant adverse effect on people, process, technology, data or facilities. Security incidents include, but are not limited to:

- A system or network breach accomplished by an internal or external entity; this breach can be inadvertent or malicious
- Unauthorized disclosure
- Unauthorized change or destruction of ePHI (i.e. delete dictation, data alterations not following GHVHS procedures)
- Denial of service not attributable to identifiable physical, environmental, human or technology causes
- Disaster or enacted threat to business continuity
- Information Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Examples of information security incidents may include, but are not limited to, the following:
    - **Denial of Service**: An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
    - **Malicious Code**: A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
    - **Unauthorized Access/System Hijacking**: A person gains logical or physical access without permission to a network, system, application, data, or other resource. Hijacking occurs when an attacker takes control of network devices or workstations.
    - **Inappropriate Usage**: A person violates acceptable computing use policies.
    - **Unplanned Downtime**: The network, system, and/or applications are not accessible due to any unexplainable circumstance causing downtime (e.g., system failure, utility failure, disaster situation, etc.).
    - **Multiple Component**: A single incident that encompasses two or more incidents (e.g., a malicious code infection leads to unauthorized access to a host, which is then used to gain unauthorized access to additional hosts).
- Other examples of observable information security incidents may include, but are not limited to:
    - Use of another person's individual password and/or account to login to a system.
    - Failure to protect passwords and/or access codes (e.g., posting passwords on equipment).
    - Leaving workstations unattended while actively signed on.
    - Installation of unauthorized software.
    - Falsification of information.
    - Theft or loss of equipment or software.
    - Destruction or tampering with equipment or software.
    - Posting of PHI on the Internet i.e. Facebook, Twitter.

- Discarding of PC hard drives, CDs or other devices including PHI without following approved destruction/disposal guidelines. (Media Disposal Policy)
- Terminated workforce member accessing applications, systems, or network.

Procedures:
The security incident response process that follows reflects the process recommended by SANS, an industry leader in security (www.sans.org).

I. *Identification Phase:*

A) Immediately upon observation workforce members report suspected and known events, indications, and security incidents in one of the following:
   - i) Report through technical means, such as the IT Help Desk.
   - ii) Direct report to management, the HIPAA Security Officer, Privacy Officer, or other.
   - iii) Email.
   - iv) Calling the Anonymous Compliance Hotline at 845-333-(HERO) 4376. (Please note the hotline is not monitored 24x7)

B) The individual receiving the report facilitates completion of an Information Security Incident Report form (Appendix 2) and notifies the HIPAA Security Officer or CIO (if not already done).

C) The HIPAA Security Officer determines if the issue is an indication, event, or security incident.
   - i) If the issue is an event or indication the HIPAA Security Officer forwards it to the appropriate resource for resolution.
     - (1) Physical Intrusion: Facilities manager, Security Department or law enforcement (if necessary for protection).
     - (2) Non-Technical Event (minor infringement): the HIPAA Security Officer investigates the incident.
     - (3) Technical Event: Assign the issue to an IT resource for resolution. This resource may also be a contractor or outsourced technical resource, in the event of lack of expertise in the area.
   - ii) If the issue is a security incident the HIPAA Security Officer notifies the appropriate IT staff and senior management if necessary.
     - (1) If a non-technical security incident is discovered the delegated IT staff member(s) completes the investigation, implements preventative measures, and resolves the security incident.
       - (a) Once the investigation is completed, progress to Phase V, Follow-up.
     - (2) If the issue is a technical security incident, commence to Phase II: Containment. Note: If there is no internal expertise to assist with security incident response request an outside vendor to assist with the technical work. Identify potential partners for this work prior to discovery of a security incident.

II. *Containment Phase (Technical):* In this Phase, GHVHS Information Technology Department (or IT consultant) attempts to contain the security incident.

A) The appropriate IT staff reviews any information that has been collected by the HIPAA Security Officer or any other individual investigating the security incident.

B) The IT staff member secures the physical and network perimeter.

C) The Information Technology department performs the following:
   - i) Load a trusted shell.
   - ii) Retrieve any volatile data from the affected system.
   - iii) Determine the relative integrity and the appropriateness of backing the system up.
   - iv) If appropriate, back up the system.
   - v) Change the password(s) to the affected system(s).
   - vi) Determine whether it is safe to continue operations with the affected system(s).
     - (1) If it is safe, allow the system to continue to function;

(a) Complete any documentation relative to the security incident on the Information Security Incident Report Form.
(b) Move to Phase V, Follow-up.
(2) If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.

III. *Eradication Phase (Technical):* The Eradication Phase represents the Information Technology Departments effort to remove the cause, and the resulting security exposures, that are now on the affected system(s).

A) Determine symptoms and cause related to the affected system(s).
B) Strengthen the defenses surrounding the affected system(s), where possible (a risk assessment may be needed). This may include the following:
i) An increase in network perimeter defenses.
ii) An increase in system monitoring defenses.
iii) Remediation of any security issues within the affected system, such as removing unused services/general host hardening techniques.
iv) Others.
C) Conduct a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed.
i) If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.
D) Update the Information Security Incident Report Form with the information learned from the vulnerability assessment, including the cause, symptoms, and the method used to fix the problem with the affected system(s).
E) Apprise Senior Management of progress.
F) Move to Phase IV, Recovery.

IV. *Recovery Phase (Technical):* The Recovery Phase represents the Information Technology Departments effort to restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected.
A) The technical team determines if the affected system(s) have been changed in any way.
i) If they have, the technical team restores the system to its proper, intended functioning ("last known good").
(1) Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).
(2) If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behavior.
ii) If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.
B) Update the Information Security Incident Report Form with the detail that was determined during this phase.
C) Apprise Senior Management of progress.
D) Move to Phase V, Follow-up.

V. *Follow-up Phase (Technical and Non-Technical):* The Follow-up Phase represents the "hot wash" of the security incident to look for "lessons learned" and to determine whether the process that was taken could have been improved in any way. It is recommended all security incidents be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks post-incident.
A) Responders to the security incident meet to review the documentation collected during the security incident.
i) Create a "lessons learned" document and attach it to the completed SIR Form.
ii) Determine what could be improved.

iii) Communicate these findings to Senior Management for approval and for implementation of any recommendations made post-review of the security incident.
iv) Carry out recommendations approved by Senior Management.
v) Close the security incident.

B) Periodic HIPAA and Technical Evaluation:
i) It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding GHVHS's expectation for them, relative to security responsibilities.

VI. *Retention of Security Incident Documentation:* Maintain all documentation surrounding every security incident, to include all work papers, notes, incident response forms, meeting minutes and other items relevant to the investigation in a secure location for a period of two (2) years

Compliance:

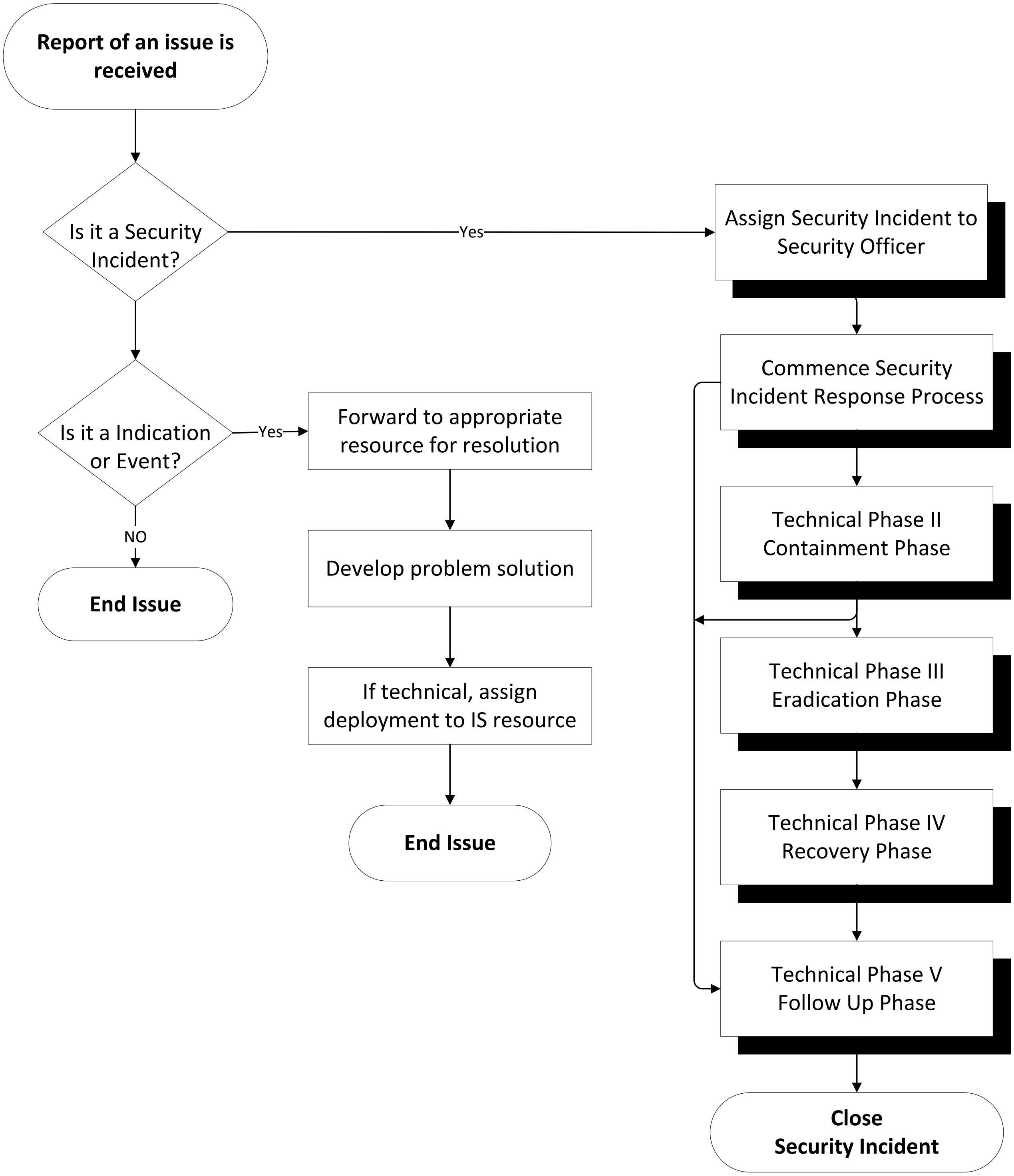
Failure to comply with this or any other security policy will result in disciplinary actions up to and including termination.

Security Incident Procedures is a standard (164.308 (a)(6)) defined in the Administrative Safeguards category of the HIPAA Security Rule.

References:

- SANS (SysAdmin, Audit, Network, Security) Institute, Sample Incident Handling Forms,
- "Security Incident Response," HIPAA COW Presentation, Eric Sinclair, CISSP, Information Security Specialist, United Government Services, September, 2004
- NIST Computer Security Incident Handling Guide, Special Publication 800-6
- GHVHS HIPAA Breach & Discipline Policy

APPENDIX 1: SECURITY INCIDENT RESPONSE FLOW


Report of an issue is received
Is it a Security Incident?
Yes
Assign Security Incident to Security Officer
Commence Security Incident Response Process
Is it a Indication or Event?
Yes
Forward to appropriate resource for resolution
Technical Phase II Containment Phase
NO
End Issue
Develop problem solution
Technical Phase III Eradication Phase
If technical, assign deployment to IS resource
Technical Phase IV Recovery Phase
End Issue
Technical Phase V Follow Up Phase
Close Security Incident

APPENDIX 2: INFORMATION SECURITY INCIDENT REPORT FORM

INCIDENT IDENTIFICATION INFORMATION[1]

Incident Detector's Information:

Name:	Date/Time Detected:
Title:	Location:
Phone/Contact Info:	System/Application:

INCIDENT SUMMARY

Type of Incident Detected:

- □ Denial of Service
- □ Unauthorized Access
- □ Malicious Code
- □ Unplanned Downtime
- □ Unauthorized Use/Disclosure
- □ Other:

Description of Incident:

How was the Incident Detected:

Names of Others Involved:

INCIDENT NOTIFICATION

- □ IT Leadership
- □ Administration
- □ Human Resources
- □ Compliance
- □ Other:
- □ System/Application Owner
- □ System/Application Vendor
- □ Public Affairs
- □ Legal Counsel

ACTIONS (Include Start & Stop Times)

Identification Measures (Incident Verified, Assessed, Options Evaluated):

Containment Measures:

Evidence Collected (Systems Logs, etc.):

[1] This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only

Eradication Measures:		
Recovery Measures		
FOLLOW-UP		
Review By (Organization to determine)**:**	□ Security Officer	□ IT Department/Team
	□ Other:	
Recommended Actions Carried Out:		
Initial Report Completed By:		
Follow-Up Completed By:		