


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-22	1 of 5
TITLE: RESPONSE AND REPORTING POLICY				

PURPOSE:

The purpose is to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the Guam Memorial Hospital Authority; and document security incidents and their outcome. This is a standard required under the Administrative Safeguards of the HIPAA Security Rule.

SCOPE:

This policy applies to Guam Memorial Hospital Authority in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit ePHI.

POLICY:

This policy requires addressing the following seven steps:

1. Preparing for a Security Incident
2. Detecting and Reporting Security Incidents
3. Assembling the Incident Response Team
4. Limiting Further Damage
5. Gathering Evidence
6. Fixing the Damage
7. Analyzing the Incident

Step 1: Preparing for a Security Incident

Every network will at some point be a victim of a computer security incident. System and network administrators must be prepared for security incidents and be able to respond quickly to minimize and repair the damage. Some critical steps that must be addressed are:

- Identify the Security Incident Response Team
- Acquire specialized security training
- Verify the deployment of Intrusion Detection Systems (IDS)
- Verify Data Backup Plan and its implementation

The key is to be prepared so that in the event of a security incident the response is swift and comprehensive in resolving the damage.

Reviewed: 01/2006
Revised: 02/2006
Approved: EMC 2/15/06

Step 2: Detecting and Reporting Security Incidents

As soon as security incidents are detected they should be immediately reported using the Security Incident Form to the HIPAA Security Officer or the Security Incident Response Team.

A formal reporting procedure should be established, together with an incident response procedure, setting out the action to be taken on receipt of an incident report. All employees and contractors should be made aware of the procedure for reporting security incidents, and should be required to report such incidents as quickly as possible. Suitable feedback processes should be implemented to ensure that those reporting incidents are notified of results after the incident has been dealt with and closed. These incidents can be used in user awareness training as examples of what could happen, how to respond to such incidents, and how to avoid them in the future.

Further, all users of information services should be trained to note and report any observed or suspected security weaknesses in, or threats to, systems or services. They should report these matters either to their management or to the HIPAA Security Officer as quickly as possible. Users should be informed that they should not, in any circumstances, attempt to prove a suspected weakness. This is for their own protection, as testing weaknesses might be interpreted as a potential misuse of the system.

Procedures should also be established for reporting malfunctions such as those related to software, hardware or any other type.

Step 3: Assembling the Security Response Team

The Security Incident Response Team must meet to evaluate and determine the potential cause of the incident. The following actions should be considered by the team:

- The symptoms of the problem and any messages appearing on the screen should be noted.
- The computer should be isolated, if possible, and use of it should be stopped. The appropriate contact should be alerted immediately. The matter should be reported immediately to the information security manager.

Users should not attempt to remove the suspected software unless authorized to do so. Appropriately trained and experienced staff authorized by the Security Incident Response Team should carry out recovery activities.

Step 4: Limiting Further Damage

Once the initial data has been collected, immediate steps need to be taken to minimize the spread of the damage. These steps may include disabling Internet access as well as disabling file servers, email servers, communication devices and other systems. The workstation(s) impacted should be isolated, if possible, and their use stopped. If equipment is to be examined, it should be disconnected from any organizational networks before being re-powered. Diskettes and other media should not be transferred to other workstations.

Step 5: Gathering Evidence

The Security Incident Response Team must gather all possible evidence to fully understand the type of attack and its scope. The team needs to address questions such as:

- How many systems are impacted?
- What levels of privileges were accessed?
- How widespread is the vulnerability?
- How far into the internal systems did the intruder get?
- Which systems have been compromised?
- Any risk to ePHI stored by systems?

All of the information collected should be thoroughly documented and reported. Dedicated systems should be used for incident analysis and forensics. The involved personnel should be trained in the use of such applications.

Step 6: Fixing the Damage

Having gathered all the evidence the Security Incident Response Team must get involved in leading eradication efforts. Malicious files should be deleted, removed or replaced. User accounts and associated passwords may need to be modified or re-created – if there was any evidence of unauthorized access. Data may need to be restored from trusted backups. After the impacted systems are cleaned and protected, they may be brought back online.

Monitor these systems and the infrastructure for other similar, subsequent incidents.

Step 7: Analyzing the Incident

The Security Incident Response Team re-groups to do a post-event de-briefing. The objective is to assess the incident, the response, and identify any specific areas of concern. The team must have a full and complete understanding of the incident and how to prevent such incidents from occurring in the future.

There should also be a review of mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored. This information should be used to identify recurring or high impact incidents or malfunctions. This may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or to be taken into account in the security policy review process.

Finally, there should be a formal disciplinary process for employees who have violated organizational security policies and procedures. Such a process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures.

Incidents characterized as serious by the HIPAA Security Officer will be responded to immediately and reported to all upper-level management.

Guam Memorial Hospital Authority will attempt to mitigate any harmful effects, when possible, where a security incident affects customer or patient information.

The Guam Memorial Hospital Authority will develop security policies to identify core activities in the area of Response and Reporting implementation specification of the HIPAA Security Rule.

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for determining the appropriate level of response to a security incident. All such response must be in accordance with established policies and procedures. At a minimal, the HIPAA Security Officer and/or his/her team must immediately consider a response that includes:

- Disconnecting the affected system from the network (should not remove power from the system)
- Determining if the incident is accidental or intentional
- Identifying all system-related information such as:
 - Hardware address
 - System name
 - IP address
 - E-PHI data processed by the system
 - Applications installed on the system
 - Location of the system

Members of the workforce will immediately report any and all suspected violations of information security to the HIPAA Security Officer.

All incident reporting and response activities must be conducted strictly on a need-to-know basis.

All members of the workforce will be trained on appropriate reporting of security violations.

The Security Incident Report Form, if not completed by reporting party, should then be completed by the HIPAA Security Officer or a member of his/her team will include as much information as possible about the following:

- Contact information of the person reporting the incident (name, phone, address, email)
- Date and time of the incident
- Detailed description of the incident
- Any further information, such as unusual activities or individuals associated with the incident

COMPLIANCE:

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy 6420-8. Legal actions also may be taken for violations of applicable regulations and laws such as HIPAA.

Response and Reporting is a required implementation specification defined within the Security Incident Procedures standard (164.308 (a)(6)) in the Administrative Safeguards category of the HIPAA Security Rule.

PROCEDURES:

Procedures related to the Response and Reporting Procedure includes:

- Workforce Security Procedure
- Security Incident Procedure
- Information System Activity Review Procedure
- Information Access Management Procedure
- Password Management Procedure

REFERENCES:

- HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>, February 20, 2003.
- CMS, "CMS Information Systems Security Policy, Standards and Guidelines Handbook", CMS, February 2002.
- International Standards Organization (ISO/IEC 17799:2000(E)).