UNM HEALTH SCIENCES CENTER

Applies To: **HSC**
Responsible Office**: HSC Information Security Office**
Effective Date: 12/22/2011

Title: **HSC-270 Information Systems Activity Review**	**Policy**

Responsible Authority **Last Revision: New Policy**
Chancellor for Health Sciences
HSC Executive Compliance Committee with advice from the IT Security Council
HSC Information Security Officer (ISO) / HIPAA Security Officer

Policy Sections ……page

SCOPE

The HSC ISO Information Systems Activity Review procedures define methods to identify, track and periodically assess systems. These procedures will assist in promptly responding to IT Security incidents and promote the appropriate compliance with applicable policies and regulations for systems containing HSC information assets.

UNM Health Sciences Center policies apply to all health care components of UNM that are under the jurisdiction of the HSC as designated in UNM Board of Regents Policy 3.4 Subject: Health Sciences Center and Services and UNM Board of Regents Policy 3.7 Subject: Institutional Compliance Program.

POLICY STATEMENT

Working with the HSC Compliance Office and the HIPAA Privacy Officer, and under the direction of the IT Security Council, the HSC ISO will coordinate the development, review, and approval of Information Systems activity review procedures. These procedures will identify, track and periodically assess Critical and Basic Information Systems for compliance with all applicable laws, regulations, HSC and University policies and procedures including all HIPAA regulations.

The HSC Information Security Officer will work with other HSC offices to promptly respond to any IT Security incidents (Reference: Policy HSC-240) identified through systems activity reviews.

REASON FOR POLICY

Sound business practice as well as compliance with regulations requires appropriately protecting the integrity, availability and confidentiality of Confidential or Restricted information, including ePHI, to prevent loss of service and to comply with regulatory requirements. This policy establishes the method and requirements for assessing systems containing Confidential or Restricted information and overseeing regular systems activity reviews by local IT support groups.

POLICY SECTIONS

HSC-270.1 Identify and Track Critical Information Assets

The HSC ISO will use multiple approaches to identify information systems and shall create and maintain a process for tracking Critical Information Systems.

- The HSC shall work with the Unit Security Liaisons (Reference: HSC-200) and use other communications as proactive methods to query members of the health care components to self-identity Critical Information Systems that will be included in the Critical Information System Inventory. IT Components (i.e., System Owners, Unit Heads, and other personnel) are required to provide regular reports detailing updates and changes to their Basic and Critical Information Systems that significantly impact HSC IT Security.
- The HSC ISO shall send notices on a rotating basis as described in HSC-270.2.1 to Critical Information System Owners requiring validation or update of the required system information including critical infrastructure dependencies.
- Using the Critical Information System Inventory, the HSC ISO shall identify system entries that are incomplete, out-of-date or appear to fall outside of HSC IT Security standards and follow up with IT Components (i.e., System Owners, Unit Heads, and other personnel) to see that the information is updated or practices reviewed.
- The HSC ISO shall implement a procedure to perform an annual spot check or sampling to verify the accuracy of selected system data in the Critical Information System Inventory.

HSC-270.2 Assessing Information Systems

HSC-270.2.1 Critical Information Systems

In order to provide findings to the IT Security Council and the HSC Compliance Office, the HSC ISO shall review reports of Critical Information Systems activity and IT Security configurations on a defined periodic basis, in conjunction with any routine audits, or in response to IT Security Incidents. The frequency and scope of the required Activity Reviews (Reference: HSC-270.4) will be commensurate with each system's data criticality profile based on a self-assessment as recorded in the Critical Information Systems Inventory as follows:

- Profile I – High Data Criticality - The activity in systems whose data is profiled as High Criticality (i.e., primary source for treatment, payment, health care operation, and student or employee records) shall be reviewed on an annual basis.
- Profile II – Medium Data Criticality - The activity in systems whose data is profiled as Medium Criticality (i.e., primary source for billing or scheduling or other healthcare operations not related to treatment; or primary source for approved research study) shall be reviewed on a rotating basis not to exceed three years.
- Profile III – Low Data Criticality - The activity in systems whose data is profiled as Low Criticality (i.e., primary source of PHI for pre-research; or secondary source of PHI for research/pre-research; secondary source of PHI for treatment, payment or healthcare operations; or teaching) shall be reviewed on a rotating basis not to exceed five years.

HSC-270.2.2 Basic Information Systems

In order to provide findings to the IT Security Council and the HSC Compliance Office, the HSC ISO shall review reports of Basic Information Systems activity and IT Security configurations on a defined periodic basis, in conjunction with any routine audits, or in response to IT Security Incidents.

HSC-270.3 Avoiding IT Security Incidents

The HSC ISO will develop reporting criteria, based on the Critical Information Systems Inventory, which can be used to identify systems that deviate from policy and regulatory requirements. The HSC ISO will work with IT Components (i.e., System Owners, Unit Heads, and other personnel) to ensure that compliance is achieved. In particular, the HSC ISO will examine the procedures for review of system logs.

HSC-270.4 System Activity Review

The system activity review process shall include a review of system activity logs and reports. This process may include a review of the following types of system activity information either as a full review or as a spot check or sampling:

- IT Security incident response reports
- System user privileges grants and change logs
- User-level system access logs, if available
- User-level system activity logs, if available
- User-level transaction log reports, if available
- Unit-level exception reports

The required level of system activity logging and reporting capabilities and the actual scope of the activity review for each risk profile should differ based upon a system's assigned data criticality level. These logging capabilities and review requirements are defined in Procedure HSC-270 PR.1.

Issues identified in a system activity review will be assessed to ensure acceptable levels of risk to Unit and HSC business operations. Assessment actions include but are not limited to:

(1) the Unit classifies and reports the risk via a Unit Exception Report,
(2) the risk is reviewed based on acceptable risk profiles for the Unit and the HSC,
(3) findings of significant risk are scheduled for a coordinated resolution,
(4) findings that demonstrate an unacceptable impact on business operations are escalated to the IT Security Council for review.

DEFINITIONS

Refer to the HSC Master Glossary of IT Security Terms.

PROCEDURES

Procedure HSC-270 PR.1 Information Systems Activity Review Procedure

RELATED INFORMATION

UNM Policy 2500 Acceptable Computer Use

HSC Policy HSC-200 Security and Management of HSC IT Resources
HSC Policy HSC-210 Security of HSC Electronic Information
HSC Policy HSC-220 Information Access and Security
HSC Policy HSC-230 Electronic Data Storage and Transmission
HSC Policy HSC-240 IT Security Incident Response
HSC Policy HSC-250 Systems and Network Security
HSC Policy HSC-260 Device and Media Control
HSC Policy HSC-280 Physical Security
HSC Policy HSC-300 ePHI Security Compliance

RETIRED POLICIES SUPERSEDED BY THIS POLICY

HSC Policy 2.9 Information System Activity Review - ePHI
HSC Policy 10.1 Evaluation - ePHI

CONTACTS

Subject	Contact	Phone
IT Security Policy Matters	HSC Information Security Officer	505-272-1696
HIPAA Privacy Matters	HIPAA Privacy Officer	505-272-1493

DOCUMENT APPROVAL & TRACKING

Item	Contact	Date	Approval
Owner	Barney D. Metzner, HSC ISO, HIPAA Security Officer 272-1696		
Committee(s)	HSC Executive Compliance Committee HSC IT Security Council		Y
Legal (Required)	Scot Sauder, Senior Associate University Counsel-- Health Law Section Leader, Office of University Counsel		Y
Official Approver	Dr. Paul Roth, Chancellor for Health Sciences		
Official Signature		Date: 12/22/2011	
Effective Date:		12/22/2011	
Origination Date:		4/2011	
Issue Date:		1/9/2012	ar

ATTACHMENTS

None.