UNM HEALTH SCIENCES CENTER

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

Title: **HSC-280 Physical Security**	**Policy**

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

Last Revision: New Policy

Policy Sections ……. page

SCOPE

This policy establishes protections against unauthorized physical access to HSC IT Assets. This includes protected health information (PHI) in electronic formats (i.e., hard drives, video, audio) and covers Confidential or Restricted information accessed on campus and on non-HSC property.

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

HSC IT Assets containing unsecured Confidential or Restricted information must be physically secured in order to prevent unauthorized access.

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 legal requirements. This policy establishes the method and requirements for controlling the physical access and security of devices that contain HSC Information Assets.

DEFINITIONS

Refer to the HSC Master Glossary of IT Security Terms.

POLICY SECTIONS

HSC-280.1 Physical Access to Data Centers and Critical System Areas

All locations with HSC Information Assets must be adequately protected from physical access by unauthorized individuals. It is the responsibility of department management to implement safeguards such that Confidential or Restricted information within departments is protected

from physical access by unauthorized individuals. Additionally, environmental safeguards will be in place to protect the confidentiality, integrity and availability of information as commensurate with data criticality and risk assessment.

HSC Components are responsible for maintaining Physical Facility Security Plans for Data Centers and Critical System Areas. This Physical Facility Security Plan ensures that Confidential or Restricted information in any format (e.g., tapes, radiography, video or text on flash or optical media, etc.) that is housed in a Data Center or Critical System Area location meets business, legal and regulatory requirements for physical security. Business process owners will provide the CIO a list of Data Centers and Critical System Areas for space they control. A copy of each Physical Facility Security Plan will be provided to the HSC ISO for review and inclusion into an official Master List of Data Centers and Critical System Areas for the HSC. Final approval for Data Centers and Critical System Areas rests with the appropriate CIO or equivalent.

N.B. Workforce members, including but not limited to vendors and contractors, must physically secure information assets off campus to the same degree that information assets are secured on campus.

Individuals are responsible for securing physical access to devices containing Confidential or Restricted information maintained at a non-HSC location or on non-HSC owned equipment.

HSC-280.2 Physical Security of Portable Electronic Devices
Portable electronic devices used to create, access, store or transmit Confidential or Restricted information will be subject to special requirements (including but not limited to HSC mobile device security standards and other department-specific requirements) designed to minimize the risk of inappropriate disclosure of ePHI through theft or accidental loss.

HSC-280.3 Safeguards to the Physical Environment for the Protection of HSC IT Assets
In areas where the public may enter or where access or viewing of Confidential or Restricted data may occur, reasonable adjustments to the physical environment to reduce or prevent unauthorized access or viewing must be in place. Other controls, such as screensavers and timeouts, may be necessary to ensure that the inappropriate access or viewing of the display screen of any computing device that creates, accesses, stores or transmits Confidential or Restricted information is minimized. Compliance is paramount in patient areas, research-subject areas, employee and student records areas or when accessing information from public areas.

PROCEDURES

Procedure HSC-280 PR.1 Physical Facility Security Plan for HSC Data Centers and Critical System Areas

Procedure HSC-280 PR.2 Safeguarding Work Areas

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-270 Information Systems Activity Review
HSC Policy HSC-300 ePHI Security Compliance

RETIRED POLICIES SUPERSEDED BY THIS POLICY

HSC Policy 2.2 IT Component of the Facility Security Plan - ePHI
HSC Policy 4.2 Facility Access Controls - 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		Y
Official Signature		Date: 12/22/ 2011	
Effective Date:		12/22/2011	
Origination Date:		4/2011	
Issue Date:		1/9/2012 ar	

ATTACHMENTS

None.