UNM HEALTH SCIENCES CENTER

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

Title: **HSC-250 Systems and Network Security**	**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

---

SCOPE

This policy establishes IT security requirements for HSC workforce members and other individuals who use computing or communications systems during the course of their work at the HSC. This includes systems used on-campus as well as from remote locations, such as home, hotels and other off-campus locations.

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

This policy defines HSC standards for managing computing and communications systems and access to HSC's data network and electronic data resources. All Confidential or Restricted information including electronically stored information must be protected in a manner commensurate with its sensitivity, value and criticality; this includes protecting computing and communications systems containing that data accordingly. Safeguards regarding confidentiality and privacy of the HSC information apply equally at on-campus locations and at any remote location. Procedures associated with this policy establish currently required and best practices for managing computing and communications systems and network access.

The HSC may, at any time, change any or all of the conditions under which any individual is granted computing or communications systems or data network access privileges and may terminate such privileges at any time.

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 connecting to the HSC network to use HSC business systems.

DEFINITIONS

Refer to the HSC Master Glossary of IT Security Terms.

POLICY SECTIONS

HSC-250.1 Use and Configuration of Computing or Communication Systems

Appropriate procedures (Reference: Procedures section of this policy) regarding confidentiality and privacy of information are to be followed at all times regardless of location or device ownership.

HSC-250.2 Network Security for Individuals Who Transmit or Receive Confidential Information

Compliance with the associated procedure (Reference: Procedure HSC-250 PR.1) is specifically required for individuals who transmit or receive Confidential Information on computing or communications systems over the HSC networks.

HSC-250.3 Remote Access to HSC Data Network and Systems

It is the responsibility of HSC workforce members to ensure that their remote access connection complies with the same security requirements as the user's on-site connection. Software may be used to verify compliance with current HSC workstation standards before access is granted.

- Encryption from end to end is required for transmission of Confidential information. (Reference: Policy HSC-230)
- The workstation on the HSC network must be configured so that authentication compliant with HSC Password Standards is required, and only authorized users are allowed access.
- Remote devices connecting to HSC systems must meet the minimum requirements of the baseline standards defined in HSC-210.1.

HSC-250.4 Access to the HSC Data Network for Individuals Not Affiliated with the HSC

Individuals not associated with the HSC (including but not limited to vendors, contractors, and research collaborators) with remote access privileges must utilize a secure access method. Such individuals working with ePHI must be covered by a Business Associate Agreement, which contains text approved by University Counsel, specifying HIPAA compliance requirements before remote access will be granted.

Individuals not associated with the HSC (including but not limited to vendors, contractors, and research collaborators) with HSC Data Network access privileges must utilize a secure

method for access that provides security that is equivalent to or better than the security of the HSC Virtual Private Network (VPN) connection, and be able to provide documentation of those methods.

SPECIAL SITUATIONS

HSC departments or units may establish practices and procedures that apply specifically to that department or unit, provided that the practice or procedure is consistent with HSC policy and requires equal or greater security for Confidential or Restricted information than that required by the appropriate HSC policies.

PROCEDURES

Procedure HSC-250 PR.1 Systems and Network Security Procedures

Procedure HSC-250 PR.2 Disposal of Obsolete Computer Hardware and Peripherals

Procedure HSC-250 PR.3 Remote Access to the HSC Data Network and Systems

RELATED INFORMATION

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-260 Device and Media Control
HSC Policy HSC-270 Information Systems Activity Review
HSC Policy HSC-280 Physical Security
HSC Policy HSC-300 ePHI Security Compliance

RETIRED POLICIES SUPERSEDED BY THIS POLICY

HSC Policy 5.1 Integrity - ePHI
HSC Policy 5.2 Integrity Controls - ePHI
HSC Policy 5.3 Mechanism to Authenticate Electronic Protected Health Information (ePHI)
HSC Policy 6.4 Protection from Malicious Software - ePHI
HSC Policy 7.1 Workstation Use and Security - 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.