UNM HEALTH SCIENCES CENTER

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

Title: **HSC-220 Information Access and 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 requirements for HSC workforce members regarding access to HSC information as well as the responsibilities for stewardship of HSC information. HSC information is all information generated or acquired, in printed or electronic form, by HSC workforce members and others engaged on behalf of the HSC in the course of carrying out the mission or conducting the business of the HSC.

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

Health Sciences Center (HSC) information shall be used only for appropriate HSC purposes. HSC information is a resource analogous to an HSC financial resource or an HSC physical resource. All HSC workforce members are expected to be aware of their obligations to protect HSC information. In particular:

- HSC information that is Confidential or Restricted may not be accessed by or disclosed to anyone who does not need the information to perform the activities and fulfill the responsibilities associated with his or her HSC position. (See Policy HSC-210 for data classification details.)
- Those authorized to access Confidential or Restricted HSC information are responsible for properly storing and securing it from unauthorized access, as well as for securing and protecting passwords, keys, and other forms of access control.
- Those authorized to grant or revoke access to HSC information (as specified in Procedure HSC-220 PR.1 through PR.3) are responsible for following procedures to ensure that access is appropriately assigned, modified, and recorded as needed, and canceled promptly when a workforce member's role changes, or the workforce member transfers to another position or leaves the HSC.
- Privacy and security requirements apply to all locations, e.g., office, home, wireless. Access to Confidential or Restricted data must be limited to those users with a legitimate business need to

access the information. Appropriate safeguards must be in place to prevent unauthorized exposure of Confidential or Restricted information at all times.

- Misuse of HSC information will be regarded with utmost seriousness. Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for workforce members, and when indicated, sanctions up to and including discharge or dismissal will be imposed.

Additionally, certain categories of information, such as Protected Health Information (PHI) and student records are accorded confidentiality under applicable Federal or state regulations as well as under HSC policy. Examples include PHI which is covered by the Health Insurance Portability & Accountability Act (HIPAA) when used by a covered entity (Reference: Policy HSC-300), and student information which is covered by the Family Educational Rights and Privacy Act (FERPA), and other applicable Federal and state regulations. Anyone who violates Federal or state law is personally liable for such actions under the law as well as under applicable HSC policies.

Violations of this policy must be reported to the Data Steward responsible for authorizing access to the affected HSC system and/or information, and to the HSC Information Security and Privacy Officers or the HSC Compliance Office.

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 authorizing and revoking access to HSC information assets.

DEFINITIONS

Refer to the HSC Master Glossary of IT Security Terms.

POLICY SECTIONS

220.1 Authorization to Grant or Revoke Access to HSC Information

The following HSC officials are authorized to grant or revoke access to HSC information:

Type of Information	Official Authorized to Grant or Revoke Access
Protected Health Information (Clinical or Research)	Chief Medical Information Officer
Non-ePHI Information	See HSC Policy HSC-210 for Data Steward roles, responsibilities, and procedures

PROCEDURES

Procedure HSC-220 PR.1 HSC NetIDs and Identity Management

Procedure HSC-220 PR.2 Enterprise Account and Access Management

Procedure HSC-220 PR.3 IT Support Accounts (i.e., Service, Administrative, Vendor)

RELATED INFORMATION

UNM Policy 2500 Acceptable Computer Use
UNM Policy 2520 Computer Security Controls and Guidelines

HSC Policy HSC-200 Security and Management of HSC IT Resources
HSC Policy HSC-210 Security of HSC Electronic Information
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-280 Physical Security
HSC Policy HSC-300 ePHI Security Compliance

RETIRED POLICIES SUPERSEDED BY THIS POLICY

HSC Policy 4.1 Information Access Management - ePHI
HSC Policy 4.3 Access Control - ePHI
HSC Policy 4.4 Access Control and Validation – ePHI (Procedure)
HSC Policy 4.5 Information Access Authorization, Establishment, and Modification - ePHI
HSC Policy 4.6 Person or Entity Authentication - ePHI
HSC Policy 4.7 Unique User Identification - ePHI
HSC Policy 4.8 Automatic Logoff - ePHI
HSC Policy 4.9 Emergency Access Procedure – ePHI (Procedure)
HSC Policy 6.2 Log-in Monitoring - ePHI
HSC Policy 6.3 Password Management - 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:		1/9/2011	

ATTACHMENTS

None.