UNM HEALTH SCIENCES CENTER

Applies To: **ALL HSC**
Responsible Department: **HSC IT Security Office**
Revised: New document 6/2010

Title: **HSC-210 Security of HSC Electronic Information**	**Policy**

POLICY STATEMENT

The University of New Mexico Health Sciences Center (HSC) expects all institutional information stewards and custodians who have access to and responsibilities for electronic HSC administrative, research, student and patient information to manage it according to the rules regarding storage, disclosure, access, classification of information and minimum privacy and security standards as set forth in this policy.

DETAILED POLICY STATEMENT

The Health Sciences Center must maintain and protect its institutional information assets, comply with applicable federal (HIPAA, FERPA, etc.) and state legislation, and maintain good security practices as a matter of public trust and confidence.

APPLICABILITY

All units of the UNM Health Science Center. All UNM workforce members who have access to HSC information systems containing administrative, research, student and patient information. Additionally, all healthcare components of UNM that are under the jurisdiction of HSC as designated in UNM Board of Regents Policy Number 2.13.4 – University HIPAA Compliance Policy.

WHO SHOULD READ THIS POLICY

All stewards and custodians of electronic HSC administrative, research, student and patient information.

POLICY AUTHORITY

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

RELATED DOCUMENTS

- UNM/HSC Documents
  - UNM Business Policies and Procedures Manual
  - UNM Faculty Handbook
  - UNMH Administration and Human Resources Policies
  - HSC Compliance and HIPAA Policies
  - Security and Management of HSC IT Resources
  - Current Policies:
    - HSC Policy 8.1, Security Incident Procedure
    - HSC Policy 8.2, Response and Reporting
    - HSC Policy 4.5, Information Access Authorization, Establishment, and Modification
    - HSC Policy 2.1, Security Management Process
    - HSC Policy 7.1, Workstation Use and Security

HSC Policy 4.11, Encryption and Decryption
HSC Unit IT Security Guidelines
UNM/HSC Training
HSC Code of Conduct; HSC Culture of Compliance
HSC HIPAA Competencies; HIPAA and Breach Notification
Other Documents:
Health Insurance Portability and Accountability Act

DEFINITIONS

The following definitions apply to these terms as they are used in this policy.

Custodian	An individual with access to and/or responsibilities for ePHI and confidential information assets. This includes anyone (a) with access to HSC institutional information, (b) who uses that information in the legitimate course of HSC business, and (c) who uses information technology systems that transmit or retain HSC institutional information.
Institutional Information Steward	An HSC office(s) with executive responsibility over HSC administrative, research, student and patient information sets.
Unit Executive	For this policy, a Unit Executive is any office in the upper levels of the HSC organizational chart (which include the following offices: executive vice president, vice presidents, and deans; or their delegates).
HSC Information Asset Classifications	Information transmitted or stored on information technology systems that serve administrative, research, student and/or patient functions of the HSC. **<u>Confidential (Level 1) Information</u>** Information that has been determined by HSC Institutional Information Stewards to require the highest level of privacy and security controls. Currently, any information that contains individually identifiable health information (one or more of the eighteen (18) identifiers found in the HIPAA Privacy Rule, that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service), is considered to be Confidential (Level 1) information. Additionally, the following data elements are considered to be Confidential (Level 1) information if maintained for any reason. • Protected Health Information • Social Security number • Credit card number • Driver's license number • Bank account number ☐ Note: The data elements that comprise the category "Confidential (Level 1) Information" are reviewed regularly by HSC institutional and unit data stewards and subject to change at any time, based upon regulation, business need, etc. Refer to the HSC Policy 2.1, Security Management Process to identify the appropriate authority. In general, health information relating and identifying specific individuals as

	patients is strictly confidential and not a matter of public record. Other Confidential (Level 1) data elements may be subject to the same limitations. **Restricted (Level 2) Information** All information, unless categorized as Confidential (Level 1) or Unrestricted (Level 3), used to conduct HSC business. **Unrestricted (Level 3) Information** Information that the HSC has made available or published for the explicit use of the general public. Units in the HSC may adopt stricter baseline standards at their own discretion. If the Units choose to do so, these additional standards (and any future updates to these standards) must be documented and reported to the HSC ISO. Nothing contained in this Policy is designed to be, or should be construed in a manner which is, in any way inconsistent with, contradictory to, or limiting of the University's policies with respect to public access to University records as set forth in UNM Board of Regents' Policy 2.17 "Public Access to University Records" and/or University Business Policies & Procedures Manual, Policy 2300 "Inspection of Public Records."

RESPONSIBILITIES

Institutional Information Steward	Categorize information into one of three categories: • Level 1: Confidential • Level 2: Restricted • Level 3: Unrestricted Establish rules for disclosing and authorizing access to administrative, research, student and patient information. Conduct annual risk assessments of privacy practices and security standards. Define data stewardship roles by assigning responsibility for unit information sets to appropriate administrative staff. (See HSC Policy 2.1, Security Management Process.)
Unit Executive	Assumes responsibility for policy compliance for the information under his or her control. Deploys procedures to comply with the Institutional Information Steward's rules for disclosing, categorizing, and authorizing access to HSC administrative, research, student and patient information. Deploys procedures for meeting minimum standards for HSC

	administrative, research, student and patient information security according to information classification based on the Baseline IT Security Requirements for All Computers, Systems, and Networks sections.
Custodian	Implement procedures for policy compliance. Execute unit's procedures for meeting minimum standards for information security according to information classification based on the Baseline IT Security Requirements for All Computers, Systems, and Networks sections. Report all incidents involving unauthorized access, as detailed in HSC Policy 8.1, Security Incident Procedure.
HSC Information Security Officer	The HSC Information Security Officer is the university officer with the authority to coordinate HSC campus information technology security, with a specific focus on Confidential (Level 1) information described in the HIPAA Security Rule. The HSC ISO reports to the IT Security Council and Executive Compliance Committee. Through direction from those committees and through consultation with KMIT Committees and other stakeholders, the HSC ISO determines technical, administrative, and physical IT security procedures and reviews them annually, at a minimum.
HSC IT Service Providers	Maintain overview responsibility for implementation of this policy. Train and educate the HSC community on this policy. Monitor technological developments, changes in the law, user behavior, and the market, and suggest updates to this policy, as appropriate.
Unit Security Liaison	Receive and address requests for exceptions to security requirements. Maintain a current list of exceptions to security requirements. Review annually all exceptions to Baseline IT Security Requirements for All Computers, Systems and Networks. Receive and maintain an inventory of all systems holding Confidential (Level 1) information.

PROCEDURES

Introduction	To safeguard the HSC's information and IT resources, the HSC IT Security Officer requires the following practices. These requirements apply to any system that is (a) used to conduct HSC business, or (b) connected to the HSC networks. These requirements, as well as the accompanying requirements for securing Confidential (Level 1) information, reflect an approach referred to as “layered defense” or “defense-in-depth.” As a community, we need to build defenses on multiple levels — network, system, application, information — so that if the integrity of one is weakened, another may still be able to provide sufficient protection. It is the sum of all these measures, and not reliance on any particular aspect of security, that will move the HSC toward a more secure IT environment. **NOTE:** Any item labeled as a “☐ Suggestion:” reflects a beneficial practice that might become a requirement at some future date.

	Privacy practices and security standards serve to preserve and protect institutional information and patient privacy. The following procedures create a separation of roles and assign appropriate responsibilities for both stewards and custodians of institutional information to meet those ends at the HSC. (See HSC Policy 2.1, Security Management Process.) The integration of information technologies in virtually every aspect of transmission and storage of institutional information requires responsible administrative, technical, and physical security practices and standards. The focus of these procedures falls mainly on the administrative and technical aspects of privacy and security practices. Institutional Information Stewards (as established by HSC Policy 2.1, Security Management Process) assume responsibility for the management practices of information under their purviews. These practices include a general inventory of the kind of information specific to their roles, classification of information into one of the three categories that this policy creates for the purposes of establishing rules for the protection of that information and, most importantly, providing up-to-date authorization for access to information. Baseline standards apply to all three HSC Information Asset Classifications (Levels 1, 2, and 3) unless otherwise specifically defined. Unit Executives have the responsibility to implement this policy within their units. Custodians must comply with the rules of this policy and the baseline standards for computer security for all data classification levels. Confidential (Level 1) and Restricted (Level 2) data must comply with the technical requirements described in this policy. While no one policy can absolutely ensure the protection of institutional information, especially in an information technology landscape where the devices, applications, rules, user behavior, market drivers, and threats change constantly, this policy does provide the HSC with a coherent plan integrating state-of-the-art administrative and logical security practices. The HSC ISO can establish additional baseline standards or modify existing standards as needed by submitting additions/modifications for approval by the IT Security Council which would, upon acceptance, submit the changes to the Executive Compliance Committee or the EVP for final approval. Units in the HSC may adopt stricter baseline standards at their own discretion. If the Units choose to do so, these additional standards (and any future updates to these standards) must be documented and reported to the HSC ISO.
Exceptions	For all computers or other IT resources that are not able to meet these security requirements, the following exception process must be followed:

	1. IT resources that cannot meet the following requirements must be identified to the appropriate Unit Security Liaison who will look for alternate methods to address the risk in question. If an alternate security solution can be found to address the specific risk, an exception is not required. 2. The Unit Security Liaison may determine a local solution in consultation with and through approval by the HSC Information Security Officer. 3. The Unit Security Liaison will maintain a list of all IT resources that require an exception or are using alternate methods. 4. Any changes to the list of exceptions and/or alternate methods must be reported to the HSC ISO. 5. On an annual basis, the Unit Security Liaison will review exceptions and/or alternate methods and will provide a complete exception report to the HSC ISO.
Policy Exemption Process	In the event that unusual circumstances create a viable reason for a department to request an exemption to policy, an official waiver must be obtained. Such a waiver of policy must be formally submitted to the IT Security Council. A formal waiver is considered only if it is fully documented, endorsed, and sponsored by at least one senior HSC official. A policy waiver that is associated with significant risk requires formal approval from the Executive Compliance Committee and/or the Executive Vice President for Health Sciences before the waiver can take effect.
Baseline IT Security Requirements for All Computers, Systems and Networks	The requirements for all computers are intended to ensure a reasonable yet effective level of security for the use of campus systems and networks. Adhering to this set of basic good practices should not prove difficult for individuals and departments. See the Baseline IT Security Requirements for All Computers section of this policy. The Baseline IT Security Requirements for All Systems and Networks intends to ensure that appropriate system and network controls are in place for a reasonable yet effective level of IT security. Adhering to this set of basic good practices should not prove difficult for IT staff and management.
Additional Encryption Requirements	Additional, more stringent, requirements apply to the storage and handling of information classified as Confidential (Level 1) information. See the "Additional Encryption Requirements for Confidential (Level 1) Information" section of this policy.
Timeline for Compliance with this Policy	Compliance with all baseline security requirements is expected for all HSC units upon promulgation of this policy. Because some departments may require additional resources in meeting the IT security requirements for Confidential (Level 1) information set forth in this policy, they will not be effective until the second quarter of the fiscal year following promulgation of this policy. Exceptions may be granted in extenuating circumstances by the Executive Vice President for Health Sciences.

STANDARD OPERATING PROCEDURES

See Associated Document: HSC 210.1 Baseline IT Security Requirements

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, Executive Vice President for Health Sciences		Y
Official Signature		Date: June 23, 2010	
Effective Date:		June 23, 2010	
Origination Date:		5/2010	
Issue Date		8/6/2010	

ATTACHMENTS

None.