UNM HEALTH SCIENCES CENTER

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

Title: **HSC-230 Electronic Data Storage and Transmission**	**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 2

SCOPE

This policy establishes standards for the electronic transmission and storage of Confidential or Restricted information and the controls that the HSC workforce members will employ to protect the security and privacy of electronic Protected Health Information (ePHI). This policy applies to email, instant messaging (IM), file transfer, file storage and any other technology that transmits or stores Confidential or Restricted information electronically.

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

To protect against unauthorized access and to maintain the integrity of the Confidential or Restricted information, reasonable and appropriate security measures shall be implemented for the transmission and storage of electronic information.

- Confidential or Restricted information may be electronically stored or transmitted only when using reasonable and appropriate security measures in accordance with this policy.
- HSC workforce members must be appropriately authorized by the data owner/data steward (Reference: Policies HSC-210 and HSC-220) in order to store or transmit Confidential or Restricted information on desktops or laptops and other portable devices or media.
- The presence of Confidential or Restricted information on desktops or laptops and other portable devices and media must be limited to an amount reasonable for operations.
- HSC workforce members should encrypt Confidential information (Reference: Policy HSC-300) that is stored on desktops or laptops and other portable devices or media according to the current encryption standards unless other safeguards have been approved by the ISO.
- HSC workforce members must assure that encrypted information is accessible and retrievable as needed for operations and records retention purposes.

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 securing data in transmission and storage, as designated by its data classification (Reference: Policy HSC-210).

DEFINITIONS

Refer to the HSC Master Glossary of IT Security Terms.

POLICY SECTIONS

HSC-230.1 Reasonable and Appropriate Security Measures

Confidential or Restricted information may be electronically transmitted only when using reasonable and appropriate security measures in accordance with this policy. Generally, the greater the quantity, specificity or sensitivity of the information being transmitted, the more secure the means of transmission must be. Information that could be used to identify the individual may only be transmitted electronically using Secure Electronic Messaging, except for unusual emergency circumstances with no feasible alternative mode of communication (Reference: Procedure HSC-230 PR.2). See guidelines for handling of emergency circumstances (Reference: Procedure HSC-230 PR.3).

HSC-230.2 Data in Storage and Data in Transit

Encryption of files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks, is encouraged at all times and may be required. The HSC makes available software and protocols endorsed by the HSC IT Security Council that provide robust encryption, as well as the capability for properly designated HSC officials to decrypt the information, when required and authorized. Users encrypting information are encouraged to use only the endorsed software and protocols. Users who elect not to use endorsed encryption software and protocols on IT Systems are expected to decrypt information upon official, authorized request.

If the data is primary source PHI-Protected Health Information for TPO (treatment/payment/operations) or primary source PHI for approved research or pre-research, the only allowable methods for encryption are the officially endorsed HSC implementations as detailed in procedures listed in this policy (Reference: Procedure HSC-230 PR.1).

SPECIAL SITUATIONS

Units of the HSC may establish practices and procedures that apply specifically to that unit provided that the practice or procedure is consistent with HSC policy and requires equal or greater security for ePHI as determined by the HSC ISO.

PROCEDURES

Procedure HSC-230 PR.1 Endorsed Encryption Implementation

Procedure HSC-230 PR.2 Communication of PHI via Secure Electronic Messaging

Procedure HSC-230 PR.3 Data Handling Procedures and Guidelines

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-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 4.10 Encryption - ePHI
HSC Policy 4.11 Encryption and Decryption - ePHI
HSC Policy 4.12 Transmission 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.