UNM HEALTH SCIENCES CENTER

Applies To: **All HSC Workforce Members**
Responsible Department: **Information Technology**
Revised: **New**

Title: **Remote Access to ePHI**	**Standards and Guidelines**

DESCRIPTION/SCOPE

This standard establishes rules and guidelines for remotely accessing Health Sciences Center (HSC) systems that contain electronic Protected Health Information (ePHI). Additionally, it establishes, account, logging, data handling and remote device rules for systems allowing remote access to ePHI.

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.

REFERENCES

This standard supports compliance with the HIPAA through the implementation of HSC Policies, including but not limited to: HSC-300 ePHI Security Compliance, HSC-220 Information Access and Security and HSC-210.1 Baseline IT Security Procedures.

DEFINITIONS

Remote access is defined by the HSC as any device that connects to the HSC data network from a non–HSC controlled network, for example: DSL, cable modem, or a cellular network, using a computer, smartphone or other device. (See HSC Network Standards for devices connecting to the HSC internal business network.)

REMOTE ACCESS STANDARDS

1. Authorization Standards

1.1. HSC information shall be used only for appropriate HSC purposes when authorization for access has being granted in accordance with Policy HSC-220 Information Access and Security. Remote access to HSC systems and applications containing ePHI is a privilege granted to individuals authorized to access ePHI who are in compliance with these standards. The ability to remotely access systems with ePHI may be revoked for failure to follow these standards and procedures specified here for compliance with Policy HSC-300 ePHI Security Compliance.

1.2. Procedural steps for remotely accessing HSC enterprise or component level applications (e. g., SOM, CON, etc.) that contain ePHI are provided by the UNMH IT and HSLIC IT service providers.

1.3. Procedural steps for remotely accessing department or Unit level applications are developed and maintained by the application administrator and must be reviewed by IT security and approved by department leadership.

1.4. All users granted remote access to systems containing ePHI must be properly documented and reviewed according to procedures specified by the application administrator.

1.5. Authorization for remote access confidential and restricted data, other than ePHI, must also be managed to limit access to only those user IDs which require such access and are properly authorized by a Unit Manager.

2. Device Standards

2.1. Compliance with HSC-210.1 Baseline Security Procedures is a minimum requirement for remote access to HSC systems containing ePHI.

2.2. At minimum all data transmissions must be encrypted between the remote device and HSC systems containing ePHI. See HSC Encryption Standard.

2.3. Additional standards specifying hardware, operating system, network interface, applications, encryption or other security controls can be established by the application administrator to meet the data owner's security requirement for the ePHI classification.

2.4. Upon discovery of new threats with unacceptable risks, administrative and technical controls may change without notice at the data owner or application administrator's request.

3. Account Standards

3.1. A properly authorized account manager must manage the life cycle of accounts and roles that allow remote access to ePHI including: create, update, set password, move, group, rename delete, enable and disable.

3.2. Account managers granting remote access to applications containing ePHI must maintain a list of applications and users granted remote access to those applications that can be reviewed by the HSC Information Security Officer as requested.

3.3. All accounts used for remote access will be assigned one of the following account types

- System, application or platform Administrator
- Information user (specific user role should be identified as appropriate)

3.4. Access rights for a user (and hence userID) must be updated any time the user changes roles or job functions. It is the responsibility of the department to advise the organization of a user's change in role or job function.

3.5. Accounts granting remote access must be authorized by the Application Administrator and restrict access where possible to only data elements needed for remote access. Account restrictions may include some or all of the following,

- Limiting access to datasets and types
- Limiting access to certain systems with ePHI
- Limiting transaction types, frequencies, or amounts
- Limiting times of access

3.6. Remote devices accessing applications with ePHI will be subject to one or all of the following: automatic network disconnect, application level account logout, or password screen lock, after 30 minutes of inactivity.

3.7. Users accessing ePHI remotely must immediately logout or password lock the device screen when it is left unattended. As an added safeguard a screen saver lock must automatically lock the devices after 15 minutes of inactive.

3.8. Application, system and/or network logs are to be maintained showing remote connections to systems containing ePHI.

4. Data Handling Standard

4.1. Remote users may not print, copy, export, or otherwise capture records containing ePHI or confidential information unless a specific agreement is in place with the Institutional Information Steward authorizing such action. (Authorization for remotely retaining ePHI must be approved by an Institutional Information Steward as defined in Policy HSC-210 Security of HSC Electronic Information, e.g., UNMH, SOM, Office of Research, or higher. See HSC Data Classification Standard for details.)

4.2. Anyone with documented permission to retain records on a remote device must follow all HIPAA Privacy requirements with regard to the use and sharing of retained data.

4.3. ePHI data copied or otherwise retained by a remote device must be encrypted to approved HSC Encryption Standards

4.4. Notes or portions of a patient record that might be retained for quality of care purposes must be limited to the minimum necessary and be properly erased or destroyed after use. See HSC Policy "Documentation of Clinical Activities by Medical Staff and House Staff"

4.5. Standard text messaging is not allowed to contain ePHI.

4.6. Remote communication tools not supported by the HSC such as, email (e.g., Gmail), instant messaging (e.g., AIM), or social media and internet applications (e.g., Dropbox, Google apps, etc.) are not to be used for conducting business containing ePHI unless reviewed by IT Security and approved in writing by the data owner.

5. Exceptions to these standards must be properly documented and reported to the HSC ISO through the Unit Security Liaison as required in Policy HSC-200 Security and Management of HSC IT Resources.

DOCUMENT APPROVAL & TRACKING

Item	Contact	Date	Approval
Owner	Barney Metzner, HSC ISO, HIPAA Security Officer		
Consultant(s)	HSC Task Force on IT Security Standards, HSC Information Security Officer		
Committee(s)	HSC IT Security Council, HSC KMIT OPS Committee		Y
Official Approver	Holly Shipp Buchanan, EdD.		Y
Official Signature		Date: 1/9/2013	
Official Approver	Glen Jornigan, UNMH IT Administrator		
Official Signature		Date: 1/9/2013	
Effective Date		1/9/2013	
Origination Date		1/2013	
Issue Date	Clinical Operations Policy Coordinator	1/28/2013	ar