UNM HEALTH SCIENCES CENTER

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

Title: **HSC-300 ePHI Security Compliance** | **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**

SCOPE

Policy sections 300.1 through 300.22 add additional requirements and reinforce related IT Security policies for all who create, access, store and transmit electronic Protected Health Information (ePHI). ePHI is individually identifiable protected health information on past, present or future health care or payment for health care.

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

The intent of HSC-300 and related HSC IT Security policies is to ensure the appropriate security of all ePHI. As part of the commitment to providing the highest quality health care, the HSC respects an individual's right to maintain the privacy and electronic security of health information including information used in clinical research. The standards for protecting an individual's health information are described in the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

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. This policy supports compliance with the HIPAA Security Rule by providing a workforce guide and requirements for implementing measures to protect electronic information systems and their data.

OVERVIEW OF HIPAA SECURITY POLICIES AND PROCEDURES

This policy presents a set of references that includes the following: a Master Reference List, Contacts, and Related Information.

The following policies and procedures form a set that work together to provide a framework addressing HSC compliance with the HIPAA Security Rule. These policies and procedures all refer to the HSC Master Glossary of IT Security Terms and other noted reference information. This policy includes references to the individual policies listed below, explaining how they interact. Keeping a copy of this policy at hand will aid in understanding HSC HIPAA Security policies and how they relate to the 200-level HSC IT Security policies.

Master Reference List

HSC IT Security Policies and Related Procedures:

HSC-200 – Security and Management of HSC IT Resources

HSC-210 – Security of HSC Electronic Information

HSC-220 – Information Access and Security – policy describing information access management

- HSC-220 PR.1 through PR.3 - procedures guiding HSC Information access management

HSC-230 – Electronic Data Storage and Transmission – policy governing electronic communications and storage of ePHI

HSC-240 – IT Security Incident Response -- policy defining how workforce members report IT Security incidents, including those involving ePHI, and how the HSC will respond

HSC-250 – Systems and Network Security – policy describing requirements for connecting to HSC networks and systems, including ePHI Systems

- HSC-250 PR.1 through PR.3 - computer security guidelines, disposal of computers, and remote access procedures

HSC-260 – Device and Media Control- policy describing the protection of devices and media containing Confidential or Restricted information, including ePHI

- HSC-260 PR.1 - procedure that describes steps for media wiping or disposal

HSC-270 – Information Systems Activity Review – policy describing how the HSC monitors and reviews the activity of systems, including those with ePHI

- HSC-270 PR.1 – procedure that guides the Systems Activity Review

HSC-280 -- Physical Security – policy describing how to maintain the physical security of

Information Systems

- HSC-280 PR.1, HSC-280 PR.2 – physical security procedures

HSC HIPAA Specific IT Security Policy
HSC-300 – ePHI Security Compliance – defines HIPAA IT Security management

DEFINITIONS

Refer to the HSC Master Glossary of IT Security Terms.

POLICY SECTIONS

HSC-300.1 Institutional Responsibility

The HSC ISO under the direction of the IT Security Council shall be responsible for coordinating the development of policies and procedures that are designed to achieve ongoing compliance with HIPAA security requirements.

HSC-300.2 Risk Assessment

The HSC ISO, in collaboration with the IT Security Council and University Counsel, shall maintain a Master Risk Assessment report derived from the institutional security risk assessments performed by each of the HSC Components as required to address HIPAA security requirements.

As outlined in Policy HSC-270, the HSC ISO shall implement a process to identify ePHI systems and categories of systems. The HSC ISO will provide procedures by which System Owners who are responsible for systems containing ePHI can be assessed for compliance with HSC security policies and procedures. (See Section 300.4 below, as well as the Related Information section.)

The HSC ISO, in collaboration with other HSC Offices, will provide a methodology for and facilitate the performance of unit and system specific security risk assessments. (See Policy HSC-270 for details.) These risk assessments will include selected Critical ePHI Systems. These risk assessments shall be documented and shall provide a baseline for subsequent reviews.

System Owners who maintain systems that create, access, store, or transmit ePHI must review all systems and applications with ePHI for which they are responsible and evaluate their vulnerabilities to threats as described in Section 300.4. Analyses must be performed to determine what technical and administrative safeguards (Policies HSC-220 and HSC-230), and physical safeguards (Policy HSC-280) are required and should be implemented.

HSC-300.3 Using Official HSC Managed Servers for ePHI

Official HSC Managed Servers, such as the network file servers provided through HSC-managed domains, used for storage of ePHI must comply with all applicable HSC IT Security policies. Official HSC Managed Servers must be used for the storage of ePHI whenever any of the following conditions apply:

- More than 500 ePHI records are stored
- Data is shared with other users

- More than 500 MB of data is stored

Exceptions must be approved by the HSC ISO. In approved circumstances, the following requirements apply:

- The computer must subscribe to an approved HSC backup service.
- The computer must be registered in the Critical Systems Inventory maintained by the HSC ISO.
- A successfully completed Security Design Review with the HSC ISO for the storage resource or system.

HSC-300.4 System Owner Responsibilities

The Unit Security Liaison will maintain a list of systems containing ePHI within the Unit and the related System Owners. The definitions and responsibilities defined below provide the means for maintaining required security controls. Specific System Owner responsibilities are defined below.

1. **Basic ePHI System**

   A Basic ePHI System is a system that is typically used by a single individual and is used to access an ePHI application. A system, even if used only by a single user, which supports storage of primary source ePHI or ePHI critical for treatment, payment or health care operations is considered a Critical ePHI System.

   System Owners responsible for Basic ePHI Systems shall:

   1) Successfully complete the HIPAA Security Training offered by the HSC.
   2) Manage the Basic ePHI Systems in accordance with HSC IT Security policies and procedures to meet baseline standards and implement safe computing practices. (See Policies HSC-200 and HSC-210, and Procedure HSC-210.1.)

2. **Critical ePHI System**

   A Critical ePHI System is a system that creates, accesses, stores or transmits:
   1) Primary source ePHI,
   2) ePHI critical for treatment, payment or health care operations, or
   3) Any form of ePHI when the host system is configured to allow access by multiple users.

   Examples include but are not limited to:

   - A personal computer with a database containing ePHI that is configured to allow access by more than one user,
   - A departmental server with file shares containing ePHI,
   - A computer system used to create, access, store or transmit ePHI that is configured to allow access by a vendor/contractor,
   - A clinical care system which contains primary source ePHI, and
   - A billing system which is critical for clinical operations.

   System Owners with responsibility for Critical ePHI Systems must:

   1. Perform a security self-assessment for Critical ePHI System(s) (as outlined in HSC-270).
   2. Evaluate the risks to the confidentiality, integrity and availability of the ePHI.

3. Determine what physical, administrative and technical safeguards may be necessary to adequately address the identified risks, based on the security self-assessment, ePHI Security policies and procedures and other HSC guidance. As appropriate, System Owners must develop, document, implement and test a Contingency Plan that includes (1) a Backup Plan (2) an Emergency mode operation plan; and (3) a Disaster Recovery Plan. (See administrative safeguards as described in Section 300.13.) These requirements are outlined in Policies HSC-220, HSC-230, HSC-280 and their associated procedures.
4. Manage the Critical ePHI System(s) in accordance with all 200-level HSC IT Security policies and all applicable HSC procedures.
5. Successfully complete the HIPAA Security Training mandated by the HSC.

As outlined in HSC-270.1, the HSC ISO shall send annual notices to Critical Information System Owners requiring validation or update of the required system information including critical infrastructure dependencies.

3. **Additional Technical Support**

Technical administrative operations on HSC ePHI systems must be provided by a qualified System Administrator. In addition to technical ability, the System Administrator role requires a thorough understanding of HSC policies as they apply to ePHI systems and applications.

System Owners with the responsibility for any ePHI systems should contact the HSC ISO for information about the needed qualifications for the System Administrator role, or contact Central IT Support regarding obtaining qualified System Administrator support.

HSC-300.5 Reporting Violations

Workforce members are required to report violations of this policy.

- Refer to Policy HSC-240 IT Security Incident Response.
- Individuals who report violations will not be subjected to retaliation or harassment.

HSC-300.6 Investigation and Enforcement

- Reported IT Security policy violations and/or other IT Security events will be investigated as defined by Policy HSC-240 IT Security Incident Response and, where appropriate, referred to the HIPAA Privacy Officer and/or other HSC/University authorities. The HSC ISO is also authorized to investigate security concerns identified through means other than a reported violation, including routine and targeted monitoring activities.
- HSC IT staff can be authorized to investigate alleged violations under the direction of the HSC ISO and/or the appropriate disciplinary authority.
- **Corrective Actions:** Violations of this policy due to insufficient training or oversight may be addressed through appropriate corrective actions. A workforce member's failure to follow corrective actions as specified by a supervisor or the HSC ISO will be referred for disciplinary action in accordance with applicable disciplinary processes and procedures.

- **Disciplinary Actions:** Workforce violations of this policy will be pursued in accordance with the applicable disciplinary processes and procedures.
- **Sanctions:** Individuals found to have violated this policy may be subject to penalties provided for in applicable University policies dealing with the underlying conduct. Violations involving ePHI may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority.
- **Legal Liability:** In addition to University disciplinary procedures, individuals found in violation of this policy may be subject to criminal prosecution, civil liability, or both.

HSC-300.7 Reporting IT Security Events (Potential Breaches)

An IT Security Event that is escalated to an Incident or is determined to be a potential or possible breach of ePHI must be reported immediately in accordance with the HSC Policy, “Responding to Breaches of Protected Health Information (“PHI”)”. For details regarding responding to any incident, refer to Policy HSC-240 IT Security Incident Response.

HSC-300.8 Documentation Requirements

A written record of an action, activity, or assessment that is required by HSC IT Security Policies, must be maintained for six (6) years from the date of its creation or the date when it was last in effect whichever is later (HIPAA Audit Retention (§164.312 (b))). Examples include Security Incident reports, Contingency Plans, policies and procedures histories and Business Associate Agreements. (Reference: HSC-240.4 and HSC-240 PR.1)

HSC-300.9 Training

All HSC workforce members must complete HIPAA Privacy and HIPAA Security Training and have a working knowledge of Policy HSC-300 Electronic Protected Health Information (ePHI) Security Compliance as appropriate. Additional training may be required by the HSC (i.e., department, project) or by individuals in a responsible role (i.e., System Owner, Data Steward) to address specific role-based training requirements (i.e., Cerner PowerChart).

HSC-300.10 Passwords

All HSC workforce members who access ePHI must use strong authentication for computer and application access and comply with the UNM and HSC password standards.

HSC-300.11 HSC Email Accounts

Only the Official HSC Email System may be used for transmitting ePHI.

- Internal business transactions containing ePHI will be limited to the minimum necessary amount of sensitive information.
- ePHI forwarded to external business associates must be in accordance with a signed Business Associate Agreement and be encrypted.
- With regard to auto-forwarding messages, users may not configure any HSC email accounts which may receive or transmit ePHI to auto-forward messages to non-HSC email accounts unless the email is encrypted in transit and the recipient is authorized to receive the data and is capable of securing the data at rest.

HSC-300.12 File Transfer

Forwarding or exchanging ePHI data files or datasets outside the HSC network must meet conditions appropriate for the protection of the data, including but not limited to:

- Compliance with HSC-250 PR.1
- The transfer is properly authorized or covered under an agreement that specifies how the data will be secured (e.g., a Business Associate Agreement (BAA)), and
- The transfer must use an approved HSC Secure File Access Technology.

HSC-300.13 Technical and Administrative Safeguards

- **Technical Safeguards**
  - System Owners responsible for ePHI data systems, applications and devices are responsible for ensuring that appropriate technical safeguards consistent with HSC policies are implemented. The adequacy of these technical safeguards shall be reviewed regularly in accordance with HSC policies and procedures. Technical safeguards include, for example, the use of antivirus software or activation of login tracking procedures where appropriate.
- **Administrative Safeguards**
  - A range of administrative safeguards is employed to protect ePHI, both at the institutional level (HSC, UNMH, UNMMG, etc.) and at the System Owner level. HIPAA Security Training is required; supervisors are responsible for ensuring compliance with HSC training requirements. The HSC ISO monitors compliance with the HIPAA Security Rule through the review of electronic information activity. The University Internal Audit department may also audit within the scope of their normal audit activities.
  - System Owners with responsibility for a Critical ePHI System must develop administrative safeguards for such systems including: (1) A Contingency Plan; (2) An Emergency Mode Operation Plan; (3) A Disaster Recovery Plan; and (4) comply with physical security as outlined in HSC-280. These plans shall be developed by the responsible System Owner or by a delegated, qualified IT support group. Templates for plans are available from the HSC ISO. The plans shall be consistent with HSC policies and procedures and shall be commensurate with the risks to confidentiality, integrity and availability of the ePHI.
  - A Health Care Component may permit a business associate to create, access, store or transmit ePHI for business purposes only when a Business Associate Agreement that contains all of the requisite assurances has been entered into with the business associate.

HSC-300.14 Storing ePHI

Files containing ePHI must be properly secured:

- Stored data that has not been encrypted according to official HSC encryption standards or other standards approved by the HSC ISO must not be stored on local drives and/or mobile devices and/or media.
- The data owner/steward may request an exception through the HSC ISO.
- The loss or theft of any stored data that has not been secured (i.e., encrypted) according to official HSC encryption standards or other standards approved by the

HSC ISO must be handled according to HSC-300.7 Reporting IT Security Events (Potential Breaches).

HSC-300.15 Removal of ePHI
ePHI must be securely removed when no longer needed or when equipment is retired, including but not limited to: computers, data storage components, smartphones and other mobile devices such as thumb drives. Refer to Policy HSC-260 and related procedures.

HSC-300.16 Computing Device Configuration Standards
All computing devices used to create, access, store or transmit ePHI must be configured according to the HSC standards as defined by this policy and Procedure HSC-210.1. The system configuration standards are divided into two categories. Each category covers Basic ePHI Systems and Critical ePHI Systems respectively. These categories serve to proportionally apply available IT security resources and allow for usability features to be developed so that risks to ePHI are minimized.

Workforce members maintaining systems that store, process or transmit files containing ePHI are subject to the highest IT Security standards. The primary tool and standards used to protect such systems is the full disk encryption tool provided by the HSC. Systems that access ePHI solely by using remote control applications or authorized clinical applications (i.e., Cerner PowerChart) need to meet the IT security requirements specified by the System Owner/Data Steward.

HSC-300.17 Remote Access
When a device is not connected to the internal HSC Data Network (whether physically on- or off-campus) and directly accesses ePHI stored on an HSC networked file system, the device must be in compliance with this policy. All HSC workforce members remotely accessing ePHI must have completed the appropriate workforce training and access agreements as required by the HSC (i.e., department, project) or by individuals in a responsible role (i.e., System Owner, Data Steward). Departments must annually request or renew signed agreements in the HSC learning management system stating that departmental staff who access, store or transmit ePHI using a mobile device agree to follow the requirements specified in HSC policy.

1. Patient Care Applications with ePHI:
   - When remote access is required to HSC applications containing ePHI (e.g., Cerner PowerChart), affected HSC workforce members must meet the requirements established by the Chief Medical Information Officer.
2. HSC-250.3 Remote Access to HSC Data Network and Systems describes:
   - workforce member responsibilities
   - encryption requirements
   - password standards, and
   - workstation configuration requirements.

   Refer to Policy HSC-250 for full details.
3. File Storage and Databases with ePHI:

    - Device owners who store ePHI on non-HSC devices, as authorized by the appropriate data owner/steward, are responsible for ensuring the implementation of appropriate technical safeguards as defined by HSC policies.
    - The HSC may provide alternate solutions if requested and available, i.e., an encrypted Managed Workstation that is configured to meet all technical requirements for remote connections to HSC ePHI resources. (Reference: Policy HSC-210 and Procedure HSC-210.1 Baseline IT Security Procedures)
4. Department- or Project-specific Requirements/Procedures
    - Departments with specific needs may request HSC ISO approval of alternate remote access authentication and encryption services.
    - For department- or project-specific remote access procedures, contact the IT local support provider or the System Owner.

HSC-300.18 ePHI and Personally-Owned or Non-HSC Devices
ePHI may not be stored on personally-owned or non-HSC devices unless the device is capable of meeting IT Security requirements as specified by this policy. Device owners who create, access, store, or transmit ePHI on non-HSC-owned devices are responsible for ensuring the implementation of appropriate technical safeguards as specified by the data owner/steward, and must follow HSC policies including Section 300.17 above.

HSC-300.19 Smartphones and Mobile Devices
Current security standards for smartphones and other mobile devices, whether HSC-issued or non-HSC-issued, that create, access, store, or transmit ePHI require that measures be taken to meet IT Security requirements as specified by this policy. Administrative controls for all non-HSC-issued devices will include, but are not limited to, a user acknowledgement of risk and responsibility as part of HSC training (See HSC-300.17 Remote Access). Technical controls, including but not limited to the following, must be implemented:

- Enable password protection
- Enable automatic screen lock
- Enable encryption
- Limit unencrypted email stored on the device

Additionally, the HSC may require a Security Design Review to address security concerns involving mobile device applications that may be used to create, access, store or transmit ePHI.

See the following related policies for additional details:
HSC-300 Section 300.17 Remote Access;
HSC-220 Information Access and Security (defines general access control requirements);
HSC-250 Systems and Network Security (discusses accessing data networks and servers).

HSC-300.20 Removable Media Devices
Thumb drives or other removable media devices used to store ePHI must comply with HSC encryption standards for the protection of ePHI. Reference Policy HSC-260 Device and Media Control for additional details. Use of removable media is discouraged and should only be used when no other reasonable solution is available and all security precautions have been taken.

HSC-300.21 ePHI in Public Areas
Content from computer monitors or other devices that possibly allow the public or non-clinic staff to view ePHI must be protected. Reference Policy HSC-280 Physical Security, sub-section HSC-280.3 Safeguards to the Physical Environment for the Protection of HSC IT Assets for additional details.

HSC-300.22 Annual Compliance
All HSC workforce members who create, access, store, or transmit ePHI must complete annual learning plan competencies and remain in full compliance with HSC IT Security policies.

RELATED INFORMATION

All HSC 200-level policies including but not limited to:

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-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

RETIRED POLICIES SUPERSEDED BY THIS POLICY

HSC Policy 2.1 Security Management Process
HSC Policy 2.3 Audit Controls - ePHI
HSC Policy 2.4 Accountability - ePHI
HSC Policy 2.5 Applications and Data Criticality Analysis - ePHI
HSC Policy 2.6 Documentation - ePHI
HSC Policy 2.7 Risk Analysis - ePHI
HSC Policy 2.8 Risk Management - ePHI
HSC Policy 2.10 Maintenance Records - ePHI
HSC Policy 2.11 Security Sanctions - ePHI
HSC Policy 3.1 Workforce Security - ePHI
HSC Policy 3.2 Authorization and/or Supervision - ePHI
HSC Policy 3.3 Workforce Clearance Procedure - ePHI
HSC Policy 3.4 Termination and Transfer Policy - ePHI
HSC Policy 4.13 Business Associates Contracts and Other Arrangements Summary - ePHI
HSC Policy 6.1 Security Awareness and Training - ePHI
HSC Policy 6.5 Security Reminders - ePHI
HSC Policy 9.1 Data Backup Plan - ePHI
HSC Policy 9.2 Disaster Recovery Plan Summary - ePHI
HSC Policy 9.3 IT Disaster and Contingency Plan - ePHI
HSC Policy 9.4 Emergency Mode Operation Plan - ePHI
HSC Policy 9.5 Testing and Revision - 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 Leadership Council, 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		Y
Official Signature		Date: 12/22/2011	
Effective Date:		12/22/2011	
Origination Date:		4/2011	
Issue Date:		1/9/2012	ar

ATTACHMENTS

None.