1.0 Purpose/Objectives.

1.1. Reduce the risk of unauthorized access to Health Sciences information, including confidential/sensitive information (e.g., electronic Protected Health Information (ePHI)) by controlling the use, storage and disposal of devices and media.

1.2. It is the Health Sciences' position that Health Science information in any form and throughout its life cycle shall be protected from unauthorized access, modification, destruction, or disclosure, whether accidental or intentional. Improper handling and disclosure of information pose significant risks to Health Sciences, including violation of federal and state laws and civil liabilities. Our goal is the added security of encryption-at-rest, since it is one of the strongest protections against unauthorized access to information. Encryption will be installed on all devices in a manner that will not impact any functionality or create any inconvenience to users.

2.0 Scope.

2.1. UNM Health Sciences policies apply to all health care components of UNM that are under the jurisdiction of the Health Sciences as designated in UNM Board of Regents Policy 3.4 Subject: Health Sciences Center (HSC) and Services and UNM Board of Regents Policy 3.7 Subject: Health Sciences Center Institutional Compliance Program and Regents' Policy Manual - Section 3.8: Institutional HIPAA Compliance Program. This includes clinical, academic, research and staff elements.

2.2. This policy applies to devices (e.g., laptops, desktops, phones) managed by the HSC and any media storing HSC data.

3.0 Content.

3.1. General Requirements for Media and Devices

3.1.1. Health Sciences devices and media containing UNM Health Sciences information shall be handled in a manner that reduces the risks of unauthorized access. Media shall be encrypted and password-protected with the password or Personal Identification Number (PIN) memorized or stored in a separate location than the device.

3.1.2. Media and devices shall be in secure locations. Properly implemented media encryption, as determined by the Health Sciences Information Security Officer (ISO), shall be considered a secure location. HIPAA data physical security requires two locks. Encrypted media requiring a password or PIN not stored with the media is functionally equivalent to this requirement.

3.1.3. Units dealing with media containing confidential/sensitive data shall follow any additional Data Owner/Data Steward requirements. Data Owners and Stewards may impose more restrictive standards, such as inventory and accountability to removable media devices or greater security for systems and media in data centers.

3.1.4. Exception Requests. The Health Sciences CIO or the UNM Hospitals Chief Information Officer (CIO) may approve exceptions to encryption-at-rest requirements. Requests shall be written, shall specify what compensatory measures will provide protection of information equivalent to encryption, and be based on at least one of these criteria:

- The system or device does not support encryption, or the addition of encryption is cost prohibitive. Request shall include a plan for replacement of the system by a specific date.
• A medical device with a demonstrated risk that encryption would affect the reliability and/or performance of the device, impacting patient care.

• A medical device in which support and/or warranty are voided by modification of the software, including the addition of encryption.

The HSC Information Security Officer shall develop a process for submitting exception requests.

3.2. Encryption at Rest for Removable Media and Portable Devices

3.2.1. Removable media (e.g., USB “flash drives”) and media on portable devices (laptops, smart phones, etc.) are especially susceptible to theft or loss. This media shall be encrypted using an encryption tool managed by Health Sciences CIO and that the Health Sciences ISO has approved.

3.2.2. The Health Sciences encryption solution shall meet U.S. Government or International Standards Organization (ISO) standards for encrypting sensitive information. The solution shall require a key (password or PIN) to open the media and a means to recover the encrypted data if the user forgets the PIN or Password.

3.2.3. Health Sciences users of removable media and devices processing/storing Health Sciences data shall not store encryption keys with the media and/or device. This requirement also applies to personally-owned devices that might store confidential or restricted data. Refer to HSC-211 Use of Personal Devices to Conduct UNM HSC Business for requirements.

3.3. Disposition, Disposal or Transfer of Media Containing Confidential or Restricted Information

3.3.1. Confidential or restricted information shall be completely removed from electronic media before reuse. (Reference: NIST Special Publication 800-88). This is normally accomplished by physical destruction or by “bit wiping” using an approved technique. Contact the Health Sciences ISO for information on proper disposition/disposal methods.

3.3.2. When use of the media is no longer required, the media must be destroyed, rendered unrecoverable or returned to the Data Owner/Data Steward. A Data Owner/Data Steward responsible for confidential or restricted data may impose more stringent security requirements, such as tracking removable media.

3.3.3. When removable media or mobile device is transferred to another user with the information intact, the transferring staff member shall verify that the receiving staff member has authorization and need-to-know for any information that will be retained on the media or device. If the information is confidential or restricted, the transferring staff member shall obtain concurrence of the Data Owner or Data Steward.

3.4. Use of Personal Removable Media for HSC Data

3.4.1. Use of personally owned media is highly discouraged. However, if a Data Owner/Data Steward decides to allow this, (s)he and the staff member shall ensure that the media is encrypted in the same manner as Health Sciences-owned portable media and devices.

4.0 Responsibilities.

<table>
<thead>
<tr>
<th>RESPONSIBILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position/Title/Group</td>
</tr>
<tr>
<td>Health Sciences</td>
</tr>
</tbody>
</table>

*PRINTED VERSIONS OF THIS DOCUMENT ARE NOT CONTROLLED AND ARE FOR REFERENCE ONLY. THE USER IS RESPONSIBLE TO CHECK THE ONLINE POLICY WEBSITE TO VERIFY THE CURRENT VERSION PRIOR TO USE.*
5.0 Records. Applicability/Retention.
Records will be managed in accordance with the applicable Health Sciences Records Policy

6.0 External Reference(s).
International Standards Organization (ISO/IEC 27002, 8.3 Media handling)
National Institute of Standards and Technology Special Publication 800-88 Guidelines for Media Handling

7.0 Internal Reference(s).
HSC Policy HSC-200 Security and Management of HSC IT Resources
HSC Policy HSC-210 Security of HSC Electronic Information
HSC Policy HSC-211 Use of Personal Devices to Conduct UNMHSC Business
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-270 Information Systems Activity Review
HSC Policy HSC-280 Physical Security
HSC Policy HSC-300 ePHI Security Compliance

8.0 Definitions.
Confidential: Information that has been determined by HSC Institutional Information Stewards to require the highest level of privacy and security controls. (See Policy HSC-210 Security of HSC Electronic Information for full details.)
Data Steward: Data Stewards are responsible for data content, context, and associated business rules.
Data Owner: A data owner has administrative control and has been officially designated as accountable for a specific information asset dataset.
Encryption: The process of converting data from plaintext to a form that is not readable to unauthorized parties, known as ciphertext.
Encryption at Rest: The encryption of data while it is stored on any medium.
Disposal or Disposition: The permanent destruction of media.
Medium/ Media: Any physical storage that contains data such as removable and non-removable hard disk drives, magnetic tapes, DVD and CD discs, USB flash drives, and all other types of removable storage.

Restricted: Information that has been determined by HSC Institutional Information Stewards to require the highest level of privacy and security controls. (See Policy HSC-210 Security of HSC Electronic Information for full details.)

Secure Location: An area or place with restricted and/or monitored physical access through card key or physical lock.

Transfer of Media: Transmit media (internally or externally in compliance with HIPAA or other applicable regulatory guidance) and the data contained therein from one party to another party that has the appropriate authorization to access and maintain the data.

9.0 Key Words.
Security, Device, Disposal, Encryption, Media Control

10.0 Attachments.
None

11.0 Approval Authority.

<table>
<thead>
<tr>
<th>Item</th>
<th>Contact Information</th>
<th>Date</th>
<th>Approved/Reviewed</th>
</tr>
</thead>
</table>
| Document Owner     | M.W. Meyer  
 | Information Security Officer  
 | Health Sciences Center Chief Information Office  
 | mwmeyer@salud.unm.edu  
 | 505.272.1696         | 06/22/2020    | Reviewed         |
| Committee          | HSC Executive Compliance Committee                      | 08/06/2020   | Reviewed         |
|                    | IT Advisory Board                                      | 05/19/2020   | Reviewed         |
| Committee          | HSC IT Security Council                                | 05/19/2020   | Reviewed         |
| Consultant         | Health Sciences Policy Manager: Gail Hammer            | 10/13/2020   | Reviewed         |
| Committee          | Health Sciences Core Team                              | 10/01/20     | Approved         |
| Official Approver  | Dr. Michael Richards, Interim Executive Vice President  
 | of Health Sciences                                           |             | Approved         |
| Official Signature | Michael Richards                                       | 10/16/2020   |                   |

12.0 Document History.
### Date and Date Type:
( Specify: Origination, Effective or Retired Date)

<table>
<thead>
<tr>
<th>New/Revision #</th>
<th>Title of Document</th>
<th>Description of Change(s)</th>
<th>Approved By: Print Name/Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>HSC-260 Device and Media Control Policy</td>
<td>Original</td>
<td>Dr. Paul Roth, Chancellor of Health Sciences</td>
</tr>
<tr>
<td>Revision 1</td>
<td>HSC-260 Device and Media Control Policy</td>
<td>Require all laptops and removable media processing HSC data to be encrypted at rest, instead of only systems processing ePHI and other confidential information. Updated document owner.</td>
<td>Dr. Michael Richards, Interim Executive Vice President of Health Sciences</td>
</tr>
</tbody>
</table>
"HS  Device and Media Control" History

Document created by Carlotta Abeyta (abeytac@salud.unm.edu)
2020-10-15 - 8:36:52 PM GMT- IP address: 64.234.175.62

Document emailed to Michael Richards (mrichards@salud.unm.edu) for signature
2020-10-15 - 8:38:40 PM GMT

Email viewed by Michael Richards (mrichards@salud.unm.edu)
2020-10-16 - 1:47:57 PM GMT- IP address: 174.56.60.44

Document e-signed by Michael Richards (mrichards@salud.unm.edu)
Signature Date: 2020-10-16 - 1:48:18 PM GMT - Time Source: server- IP address: 174.56.60.44

Agreement completed.
2020-10-16 - 1:48:18 PM GMT