Title: HSC-260 Device and Media Control

Policy

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

Last Revision: New Policy

SCOPE
This policy applies to electronic media in any format that contains Confidential or Restricted information.

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
Prevention of unauthorized access to HSC Confidential or Restricted information, including electronic Protected Health Information (ePHI), will be maintained by controlling the use, re-use, storage and disposal of media containing such information.

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 media handling to protected data from unauthorized access and disclosure.

DEFINITIONS
Refer to the HSC Master Glossary of IT Security Terms.

POLICY SECTIONS

HSC-260.1 General Guidelines for Media containing Confidential or Restricted Information
All media containing Confidential or Restricted information should be handled in a manner that prohibits unauthorized access. Units dealing with media containing Confidential or Restricted data should follow the relevant Data Owner/Data Steward media handling...
standards or create and maintain operational guidelines equal to or more restrictive than those standards.

**HSC-260.2 Disposition and/or Disposal of Media containing Confidential or Restricted Information**

Complete removal of Confidential or Restricted information from electronic media is required before the media is made available for re-use (Reference: Procedure HSC-260 PR.1).

When the use or retention period of any media containing Confidential or Restricted information is completed, the Confidential or Restricted information must be destroyed, rendered unrecoverable, or returned to the Data Owner/Data Steward. Units dealing with media containing Confidential or Restricted data should follow the relevant Data Owner/Data Steward media handling standards or create and maintain operational guidelines equal to or more restrictive than those standards.

**PROCEDURES**

Procedure HSC-260 PR.1 Disposition and/or Disposal of Media Containing Confidential or Restricted Information

**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-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

**RETIRED POLICIES SUPERSEDED BY THIS POLICY**

- HSC Policy 7.2 Device and Media Controls - ePHI
- HSC Policy 7.3 Data Backup and Storage - ePHI
- HSC Policy 7.4 Disposal - ePHI
- HSC Policy 7.5 Media Re-use - ePHI

**CONTACTS**

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Security Policy Matters</td>
<td>HSC Information Security Officer</td>
<td>505-272-1696</td>
</tr>
<tr>
<td>HIPAA Privacy Matters</td>
<td>HIPAA Privacy Officer</td>
<td>505-272-1493</td>
</tr>
</tbody>
</table>

Title: Policy HSC-260 Device and Media Control
Owner: HSC Information Security Officer
Effective Date: 12/22/2011
Doc. # 2794
DOCUMENT APPROVAL & TRACKING

<table>
<thead>
<tr>
<th>Item</th>
<th>Contact</th>
<th>Date</th>
<th>Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>Barney D. Metzner, HSC ISO, HIPAA Security Officer 272-1696</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Committee(s)</td>
<td>HSC Executive Compliance Committee, HSC IT Security Council</td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Legal (Required)</td>
<td>Scot Sauder, Senior Associate University Counsel-- Health Law Section Leader, Office of University Counsel</td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Official Approver</td>
<td>Dr. Paul Roth, Chancellor for Health Sciences</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Official Signature</td>
<td>Date: 12/22/2011</td>
<td>12/22/2011</td>
<td></td>
</tr>
<tr>
<td>Effective Date:</td>
<td></td>
<td>12/22/2011</td>
<td></td>
</tr>
<tr>
<td>Origination Date:</td>
<td></td>
<td>4/2011</td>
<td></td>
</tr>
<tr>
<td>Issue Date:</td>
<td></td>
<td>1/9/2012</td>
<td>ar</td>
</tr>
</tbody>
</table>

ATTACHMENTS
None.