I. **PURPOSE**

The UChicago Medicine (including UCMC, The Care Network and the UCM Community Health and Hospital Division) and the Biological Sciences Division of The University of Chicago (the “Organizations”) protects information and Information Assets that are the subject of legal, contractual, or enterprise confidentiality and security requirements (collectively the “Security Obligations”). This policy sets forth the procedures for safeguarding the Electronic Media, that stores Organizational information to ensure the Restricted or Information Use Only information’s privacy, security, and integrity is maintained, and to guard against the improper disclosure and access to unauthorized individual consistent with the Security Obligations.

II. **SCOPE**

This policy applies to Electronic Media that stores, processes and transmits the Organizations’ information. All Covered Individuals are subject to this policy.

The term “Electronic Media” means electronic storage material on which data is or may be recorded electronically.

III. **POLICY**

Each Organization’s Chief Information Security Officer, in consultation with the UChicago
Electronic Media Protection Policy

Medicine Privacy Program and legal counsel, determines the standards under which all information can be stored, and sets the standards and/or requirements applicable to the procurement, deployment, use and disposal of the Electronic Media.

Capitalized terms used in this policy are defined in the glossary attached. The CISOs together may change the definitions in the glossary without the approval of the Executive Cyber Risk Committee.

IV. PROCEDURES

1. Covered Individuals will use Electronic Media devices that are approved by the CISO of each Organization when using, accessing, storing, and moving Restricted and Information Use Only information. The CISOs ensure these Information Security Standards are available to all Covered Individuals.

2. The CISO of each Organization establishes controls and procedures applicable to generally available Electronic Media (e.g. thumb drives, external hard drives, hard drives, etc.) while each Information System Owner establishes controls and procedures applicable to the Information Systems under their control. Departmental and Unit Leaders insure that Covered Individuals under their supervision abide by the policies and procedures created by the CISOs and Information System Owners.

3. Electronic Media that contains Restricted or Internal Use Only information will be secured in the manner set by the CISO of each Organization (e.g. encryption, etc.) when physically moving the Restricted or Internal Use Only information (both within and outside of the Organization). The CISOs will ensure these Information Security Standards are available to all Covered Individuals.

4. Information System Owners, or IT Custodians, implement procedures that apply to the movement of hardware and Electronic Media.

5. The CISO of each Organization establishes procedures for the disposal or re-use of Electronic Media to ensure that EPHI, SSNs or Credit Card Numbers are removed from the Electronic Media before it is disposed of or made available for re-use. These procedures will include that the Electronic Media must be removed from the hardware, where feasible, prior to the hardware being disposed.

6. The Organizations’ business associate agreements will require return or destruction of Protected Health Information. The Organizations leadership will implement a program to inform third parties of the Organizations’ rights to require return or destruction of Restricted or Internal Use Only information; each Organization’s legal counsel can grant exceptions to the return or destruction requirement for a particular third party. At the direction of the Privacy Officer or CISO of each Organization, a third party will certify that it returned or destroyed the Restricted or Internal Use Only information.

7. The CISOs include the appropriate way in which to sanitize and/or dispose of Electronic Media that contains Restricted or Internal Use Only information in the content for Security Training. The CISOs will ensure these Information Security Standards are available to all Covered Individuals.
Covered Individuals can use unencrypted Electronic Media devices for the storage and use of Public information, assuming information is considered public knowledge.

The Organizations will use the Risk Based Controls below to implement the procedures.

V. **RISK BASED CONTROLS**

Core controls, designated as “C”, are mandatory and required across the operating environment. Low controls, designated as “L”, and Moderate controls, designated as “M”, shall be evaluated as defined by the impact analysis and subsequent risk analysis.

**Media Protection Policy and Procedures (MP-1 C)**

<table>
<thead>
<tr>
<th>Level</th>
<th>Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core</td>
<td>The CISO of each Organization establishes controls and procedures applicable to generally available Electronic Media (e.g. thumb drives, external hard drives, hard drives, etc.) while each Information System Owner establishes controls and procedures applicable to the Information Systems under their control, and Departmental and Unit Leaders insure that Covered Individuals under their supervision abide by the policies and procedures created by the CISOs and Information System Owners.</td>
</tr>
<tr>
<td>Low</td>
<td>N/A</td>
</tr>
<tr>
<td>Moderate</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Media Access (MP-2 CL)**

<table>
<thead>
<tr>
<th>Level</th>
<th>Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core</td>
<td>• Electronic Media will have physical access restricted to the appropriate personnel or role-holders with a business need.</td>
</tr>
<tr>
<td>Low</td>
<td>• Procedures will ensure access is restricted to physical Electronic Media inside of Information Systems.</td>
</tr>
<tr>
<td>Moderate</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Media Labeling (MP-3 CM)**

<table>
<thead>
<tr>
<th>Level</th>
<th>Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core</td>
<td>• If Restricted or Internal Use Only information stored on Electronic Media is intended to be transferred out of their Designated Secure Computing Facility, the media must be labeled in a manner whereby the physical Electronic Media can be traced back to the department or unit that owns the Electronic Media.</td>
</tr>
<tr>
<td>Low</td>
<td>N/A</td>
</tr>
<tr>
<td>Moderate</td>
<td>• Information Systems, or any physical Electronic Media removed from the Information System, shall have external labels affixed to indicate the distribution limitations, applicable security classification, and handling caveats of the information.</td>
</tr>
</tbody>
</table>
## Media Storage and Inventory (MP-4 CLM)

**Core**
- Endpoints and Mobile Electronic Media used for the storage of Restricted or Internal Use Only information, and all newly purchased mobile devices and laptops after the effective date of this policy, must be encrypted.
- Electronic Media must be controlled physically and safeguarded in the manner prescribed for Restricted or Internal Use Only information until the media are destroyed or sanitized in accordance with this policy.
- Inventory and disposition records for Information System Electronic Media must be maintained to ensure control and accountability of the information.

**Low**
- Media inventory records must contain sufficient data to effectively identify the owner, content and age of the media.

**Moderate**
- Automated mechanisms will be deployed to restrict access to Designated Secure Computing Facility, and to audit access attempts and access granted.

## Media Transport (MP-5 C)

**Core**
- Create a backup copy of Restricted information prior to movement of Electronic Media outside of the Designated Secure Computing Facility.
- When intact hardware or Electronic Media are transported outside of Designated Secure Computing Facility, Information System Owners must maintain a Chain of Custody record of the transaction.

**Low**
- N/A

**Moderate**
- Electronic Media must be encrypted with a FIPS 140-2 approved algorithm encryption stronger when physically transported.

## Media Sanitization and Disposal (MP-6 CM)

**Core**
- All Electronic Media with Protected Health Information and Personally Identifiable Information must be sanitized prior to disposal, release out of organizational control, or released for reuse.
- Disposal and sanitization procedures must be approved by the applicable Information Security Office.

**Low**
- N/A

**Moderate**
- Sanitization equipment and procedures are tested at least annually to ensure proper functionality.
### Media Use (MP-7 LM)

<table>
<thead>
<tr>
<th>Core</th>
<th>Low</th>
<th>Moderate</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>● The use of mobile Electronic Media in Information Systems will be restricted when such Media have no identifiable owner.</td>
<td>● Sanitization-resistant Electronic Media are prohibited for use in Information Systems.</td>
</tr>
</tbody>
</table>

#### VI. POLICY REFERENCES

- POL-RO Security Responsibility and Oversight Policy
- POL-AT Security Awareness and Training
- POL-SC Systems Communications and Protection Policy
- POL-SI System and Information Integrity Policy

#### VII. REFERENCES

- HIPAA Security Rules: 42.C.F.R.§164.310(d)
- NIST: Media Protection (MP)
- NIST FIPS Publication 140-2
VIII. INTERPRETATION, IMPLEMENTATION AND REVISION

Each CISO is responsible for the interpretation and implementation of this policy, and responsible for recommending revisions of this policy to the Executive Cyber Risk Committee.

Kenneth Polonsky  
Dean and EVP Medical Affairs, Biological Sciences Division

Sharon O'Keefe  
President, The University of Chicago Medical Center
### IX. Approval and Ownership

<table>
<thead>
<tr>
<th>Owner</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy &amp; Security Steering Committee</td>
<td>Policy Development Group</td>
<td>6/12/15</td>
</tr>
<tr>
<td>Approved By</td>
<td>Title</td>
<td>Date</td>
</tr>
<tr>
<td>Kenneth Polonsky, MD</td>
<td>Richard T. Crane Distinguished Service Professor, Dean and EVP for Medical Affairs</td>
<td>9/22/15</td>
</tr>
<tr>
<td>Sharon O'Keefe</td>
<td>President, University of Chicago Medical Center</td>
<td>9/22/15</td>
</tr>
</tbody>
</table>

### X. Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Review Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Version</td>
<td>9/22/15</td>
</tr>
<tr>
<td>2.0</td>
<td>Inclusion of Ingalls, editorial edits</td>
<td>9/6/2018</td>
</tr>
</tbody>
</table>