I. PURPOSE

The University of Chicago 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 is the subject of legal, contractual, or enterprise confidentiality and security requirements (collectively the “Security Obligations”)

This policy sets forth the minimum set of expectations for the use of personally-owned devices (such as phones, smartphones, laptops, and/or tablets) by Covered Individuals to access the Organizations’ Information and Information Assets.

II. SCOPE

This policy applies to Covered Individuals’ personally-owned devices used to store, process or transmit the Organizations’ information or access Information Assets.

III. POLICY

Each Organization’s CISO determines the standards under which a Covered Individual’s personally-owned device can be used for processing, storing or transmitting Organizations’ information, or access to Information Assets. All cyber security policies apply to personally-owned devices that access the Organizations’ Information Systems regardless of whether the device is owned by the Organizations, owned by the User, or owned by a third party.

Covered Individuals are permitted to use a personally-owned device (e.g. smartphone, tablet, laptop or desktop) for accessing the Organizations’ information or Information Systems. It is the Organizations’ policy to respect the privacy of each Covered Individuals’ personal device that is used for Organizational purposes. Covered Individuals are responsible for the applicable
security controls being applied to personal devices, or will respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings.

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**

All Personally Owned Devices

1. Users who access or store Restricted or Internal Use Only information on their personally-owned devices will follow the privacy and cyber security policies and procedures that apply to the Restricted or Internal Use Only information they are accessing and storing.

*Devices owned by someone other than the User may not be used to access or store the Organizations’ Information Systems or Restricted or Internal Use Only information (e.g. the use of hotel computers is not permitted for accessing email).*

2. **Covered Individuals** must:

   a. Destroy, remove and upon request return all of the Organization’s information from his/her personally-owned device once his/her relationship with the Organization ends or once he/she is no longer the owner or primary user of the personally-owned device.

   b. Remove or return all software applications licensed by the Organization when the software application or the personally-owned device is no longer used for Organizational business purposes.

   c. Not provide access to Organizational information to any third party, either by sharing the personally owned device or showing the personally owned device to a third party. E.g., Covered Individuals must not share their laptop that contains PHI with friends or family.

3. **Covered Individuals** must understand and agree:

   a. At no time do the Organizations accept responsibility for the maintenance, backup, or loss of information on a personally-owned device. It is the responsibility of the Covered Individual to ensure any backups are encrypted.

   b. The Organizations shall not be responsible for the loss, theft, or damage of a personally-owned device. This includes, but is not limited to, a device for Organizational business, on Organizations time, or during business travel. If device is lost or stolen, immediately contact the appropriate Information Security Office.
c. The Organizations at no time accepts responsibility for the security of the personally-owned device. The security of the device is the responsibility of the Covered Individual.

4. **Information System Owners and/or IT Custodians must:**
   
   a. Implement required security controls, such as encryption, on personally-owned devices when directed by the owner to configure the devices to access the Organizations’ information or Information Assets.

**Personally Owned Mobile Devices**

1. The CISOs of the Organizations have the overall responsibility for establishing and enforcing the security standards for Mobile Devices. These enforcements, whether through procedure and/or technology, can be:
   
   a. Device encryption to a User’s personally owned mobile device when that User uses that personally owned device to access Organizational Information.
   b. The rule that the personally owned mobile device is automatically erased if a User enters more than ten (10) incorrect passwords or passcodes to unlock the device.

V. **Policy References**

   POL-AC Access Control Policy
   POL-RO Responsibilities and Oversight Policy

VI. **References**

   HIPAA Security Rules: 45 C.F.R. § 164.306(a) & (b)
VII. **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
Personal Computing Device Policy

<table>
<thead>
<tr>
<th>Policy 6</th>
<th>POL-BD</th>
<th>Effective Date</th>
<th>Review Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>9/22/2015</td>
<td>9/6/2018</td>
<td>2.0</td>
</tr>
</tbody>
</table>

VIII. **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>6/14/15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approved By</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<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, RN</td>
<td>President, University of Chicago Medical Center</td>
<td>9/22/15</td>
</tr>
</tbody>
</table>

IX. **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, readability updates, editorial</td>
<td>9/6/2018</td>
</tr>
</tbody>
</table>