BACKGROUND:

Current University policy states, in part, "Employees must not store University private data on personally owned computers or other personally owned electronic devices.

• Policy is available on the University's Securing Private Data, Computers, and Other Electronic Devices page.

This policy defines the conditions where a personally or University owned smartphone or tablet, when properly configured with the University Google MDM solution, can be used to conduct University business including the use of private data.

Additionally, this document defines AHC-IS and individual user responsibilities for securing and managing mobile devices (i.e. Phones, tablets or other hand held devices). For the purposes of this policy, a mobile device is defined as an iOS or android based smartphone or tablet only. For specific support policy on Apple iPads please see policy 3060E.

SCOPE:

University of Minnesota employees in the Health Care Component (HCC) and who are part of the BAA or BAA/plus container in University GMail require enrollment. OIT and AHC-IS staff can verify which container a University employee belongs to if necessary.

PROCEDURE:

Device Enrollment

1. To enroll a mobile device in the University Google MDM solution a user must first be enrolled in University GMail. If they are not currently enrolled in GMail, they should review http://it.umn.edu/google-apps-ahc-and-hcc-accounts. They can enroll in GMail by going to mail.umn.edu, sign in with their X.500 username/password, and click on the “Sign-Up For Google” link.

2. Once enrolled in GMail, the HCC user’s mobile device should be configured according to the following guidelines:

   a. BAA (Business Associates Agreement) references anyone who might be receiving private health information (PHI) through his or her mail. Extra precautions must be put in place for security and legal reasons. If you add this account as a Google type account, ensure that you download and enable the Google Device Policy from your app store.

      i. Exchange

         1. **Server:** m.google.com
         2. **Account type:** Exchange/Corporate
ii. iCloud
   1. Setting up iCloud will allow you a remote wipe of the device in the case it is lost or stolen. It is a best practice to set up iCloud on your device. You must initiate the remote wipe.
   2. For more information on setting up iCloud on your iOS device, please go to http://www.apple.com/icloud/setup/ios.html.

iii. Passcode
   1. To ensure HIPAA compliance on your device you must set a passcode, you should be prompted to do so after you've added your University email account to your phone, however if not prompted, you can do this manually.
   2. To set a passcode on your iOS device:
      a. Go to Settings > General > Passcode Lock.
      b. Touch the Turn Passcode On option. This should automatically prompt you to set a 4 digit passcode.

NOTE: These additional steps here must be followed for people in the HCC.

3. Once the device is enrolled and properly configured, the user is required to enter a passcode on the mobile device if one is not already configured. The passcode must be at least 4 digits in length. Below are the required configurations that are set centrally via the University:

<table>
<thead>
<tr>
<th>iOS Devices (Apple)</th>
<th>Android Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 4 character numeric password,</td>
<td>• 4 character numeric password</td>
</tr>
<tr>
<td>• Auto-locks after 15 minutes of inactivity</td>
<td>• After 10 incorrect password attempts, all data is erased and device is configured to factory defaults,</td>
</tr>
<tr>
<td>• Requires passcode within 5 minutes of screen lock being enabled</td>
<td>• Auto-locks after 10 minutes of inactivity</td>
</tr>
<tr>
<td>• Encryption is enabled (enabled by default when a passcode is set),</td>
<td>• The user can remotely reset the passcode, ring the phone, or wipe the device using <a href="http://www.google.com/apps/mydevices">http://www.google.com/apps/mydevices</a></td>
</tr>
<tr>
<td>• The user can issue a remote wipe command via iCloud,</td>
<td></td>
</tr>
<tr>
<td>• Alternatively, 1-HELP can wipe the device if notified by the device owner.</td>
<td></td>
</tr>
</tbody>
</table>

**General Support Issues Once Enrolled**

AHC-IS will help, when possible, with hand-held computer devices but makes no commitment as to the ability to support or maintain the vast array of devices that are available for purchase. Any configuration or support provided must be directly related to the user's University business need (e.g., configuration of University email, University calendar, etc.).

1. When a user contacts AHC-IS requesting help with his/her mobile device, determine if they are an AHC-IS supported user.

2. If they are an AHC-IS supported user and the issue cannot be resolved over the phone, create and issue in ITASCA for the appropriate tech or give them the option of bringing the device to the AHC-IS Tech Center. Standard AHC-IS support procedures apply.
3. If they are not an AHC-IS supported user direct them to 1-HELP or their own local IT support.

4. Once enrolled, the user is responsible for initiating a remote wipe of the mobile device if it is lost or stolen to prevent a possible data compromise. The user can initiate a remote wipe of an Android device using http://www.google.com/apps/mydevices. If the device was properly configured, the user should see their phone along with a variety of options (wipe, reset pin, etc.). To wipe an iOS device, see paragraph 2.b in the previous section.

5. AHC-IS should assist the user in initiating the remote wipe if necessary by directing them to the proper links, websites, etc. If the device was not properly enrolled, the user should be directed to call their mobile carrier and report the phone/tablet lost.