Windows 7 Configuration for the *HMS Private* Wireless Network

The *HMS Private* wireless network uses a signed certificate from GeoTrust to prove the credentials of the authentication server. By default Windows requires the user to accept the certificate, even if the certificate is valid. To avoid having to accept the certificate each time you log into the *HMS Private* network the server’s certificate needs to be trusted when first connecting to the *HMS Private* Wireless Network.

**Step 1: Association**
- On the task bar, locate the network icon and click on it to display the ‘Connect to a network’ dialog (shown below)
- If unable to locate the network icon on the task bar, go to Control Panel\All Control Panel Items\Network and Sharing Center and click the link for ‘Connect to a network’
- Select HMS Private from the list, then click ‘Connect’
Step 2: Authentication

- Shortly after, a dialog will appear prompting with Radius Server and Root CA information. Click the dropdown for details if desired, or click ‘Connect’ to continue.
- **Note:** The server will be either “itcacsp01.med.harvard.edu” or “itcacsp02.med.harvard.edu” and the Root CA “GeoTrust Global CA”. Click Connect after validating this information.
- **Note:** By default, Windows will use the MED Domain login credentials if they were used to log into the computer. Otherwise, an additional prompt will appear.

Step 3: Password (Optional)

- The system may or may not provide an additional prompt for username and password. If the below prompt appears, enter your eCommons Username and Password to log onto HMS Private Wireless Network.