Institutional Handbook of Operating Procedures (IHOP)

<table>
<tr><td colspan="2">Section:</td><td colspan="2">2 – Information Technology & Web Related</td><td colspan="2" rowspan="2"><u>First Release Date:</u>
<u>08/15/2007</u></td></tr>
<tr><td colspan="2">Policy Name:</td><td colspan="2">02.10 Wireless Access</td></tr>
<tr><td colspan="2">Revision Author:</td><td colspan="2">Ty Masse</td><td rowspan="2"><u>Reviewed Date:</u>

04/09/2012</td><td rowspan="2">☑ Without Changes
☐ With Changes</td></tr>
<tr><td colspan="2">Original Author:</td><td colspan="2">Information Technology</td></tr>
<tr><td colspan="3">Approving Body:</td><td>Dates of Approval:</td><td colspan="2" rowspan="2"><u>Next Review Date:</u>
<u>04/09/2015</u></td></tr>
<tr><td colspan="3">Executive Cabinet</td><td>4/12/2012</td></tr>
<tr><td colspan="3">Chief Information Officer</td><td>04/09/2012</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="3"></td><td></td></tr>
<tr><td>Scope:</td><td colspan="5">This policy applies to all employees, students, contractors, visitors and consultants at the University of Texas Health Science Center at Tyler who access UTHSCT information resources and networks, or accessing other networks via UTHSCT network infrastructure. The policy applies to all data communication systems owned by and/or administered by the University of Texas Health Science Center at Tyler Information Technology networkteam, and mobile or stationary computing devices communicating via the campus wireless WiFi network.This policy applies to the 802.11b, 802.11g, 802.11a, and future 802.11 wireless standards.</td></tr>
<tr><td>Purpose:</td><td colspan="5">The University of Texas Health Science Center at Tyler develops and maintains appropriate mechanisms to protect the confidentiality, integrity and availability of its computerized data and information resources. The purpose of this policy is to address the securityvulnerabilities and responsibilities associated with wireless networking at the University of Texas Health Science Center at Tyler, and to establish appropriate procedures to ensure the protection of the existing data communications infrastructure.</td></tr>
</table>

<u>Provisions:</u>

The UTHSCT wireless network infrastructure is divided into two distinct networks.

1. **Secure Wireless Network:** This network provides secure authenticated and encrypted access to UTHSCT internal information such as patient data, e-mail and other applications located within the confines of UTHSCT's internal network.

2. **Guest Wireless Network:** This network provides unsecure access to the internet only. Any communications over this network that requires privacy must be done via a virtual private network (VPN) or the secure sockets layer (SSL) protocol. Access to the internal network is prohibited by design and by policy.

The Information Technology network team shall administer the wireless network infrastructure within UTHSCT and will install access points (AP's) for connecting wirelessly to the data communications network at various locations throughout the Health Science Center.

All access points shall be of a make, model and design identified and approved by the Information Technology network team. Access points will be deployed by the IT network team or approved contractor.

Users are strictly prohibited from installing their own AP's within the network. If such devices, considered as 'rogue' AP's, are discovered the Information Technology network team reserves the right to render

such devices dysfunctional by blocking access to them. Persistent relocation of rogue AP's will result in disciplinary action.

Wireless Network Interface Cards (NIC's) installed shall be on the approved list maintained by the IT network team.

While cards from other manufacturers may work, IT is not responsible for providing technical support for cards not on the approved list.

All data communications and activity within the wireless network will be considered un-trusted and un-secured unless it has met the security requirements established by UTHSCT for secure encrypted wireless communications. Users shall therefore be subject to restrictions implemented to protect the security and integrity of the data communications network if they need to access patient confidential, or UTHSCT private information including e-mail.

Access to the Internet shall be provided with minimal restriction. However, users accessing Internet services shall be subject to the terms and conditions of UTHSCT Acceptable Use Policy.

The active scanning of 802.11b/g or future form of wireless data streams for the purpose of finding weaknesses in the integrity of the system with the intent of exploiting such weakness is strictly prohibited. Promiscuous data capture for whatever reason is also strictly prohibited, unless it's required for troubleshooting purposes by IT network team.

Users shall never assume any privacy when using the Guest wireless service. It is the responsibility of the user to ensure their privacy and the protection of privileged information and/or intellectual property.

Attempts to bypass security or to damage the wireless service passively and/or actively are strictly prohibited. Any attempt to physically alter or remove Access Points by any user other than Information Technology network team or without the express consent of IT will result in disciplinary action.

Enforcement:

Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTHSCT Information Resources access privileges, civil, and criminal prosecution.