

**HEALTH QUEST
Policy and Procedure**

Policy # _____

TITLE:	Appropriate Use of Wireless Computer Network Infrastructure
DATE INITIATED:	04/19/07
DATES REVISED:	04/19/13
DATES REVIEWED:	03/27/16
REFERENCE POLICY #:	
DISTRIBUTED BY:	
RESPONSIBLE DEPARTMENTS	Administration; Information Services
MANUAL:	Administration; Information Services
FINAL APPROVAL:	
PAGE	1 of 3
REFERENCE:	HIPAA § 164.530

Health Quest

SCOPE: Health Quest has implemented a wireless computer network infrastructure (hereafter called ‘the wireless network’) within which a variety of mobile communication takes place. This policy covers all wireless data communication devices (personal computers, cellular phones, PDAs, IPADs, IPODs etc.) connected to Health Quest's wireless network. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to the Hospital’s network do not fall under the purview of this policy.

This policy governs access to and the appropriate use of the Health Quest’s wireless network at all times, including both work and non-work time, by Health Quest employees, physicians, volunteers, consultants and/or contractors.

Non-compliance with this policy is considered a serious breach of computer and network security and may result in disciplinary or legal action. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

POLICY:

General Provisions:

Users on the Health Quest’s wireless network must not run or write any computer program or process that is likely to consume significant network resources or otherwise interfere with the Health Quest’s care of patients or other business activities. Because of bandwidth and throughput limitations, users should refrain from downloading large files or streaming audio or video over the wireless network. Such activity may deprive others of access to Health Quest resources.

The Health Quest strictly prohibits copyright infringement. This includes, but is not limited to, software piracy, illegal music downloads, or offering copyrighted material to other users over the wireless network. Any violation of this nature will result in appropriate disciplinary and/or legal action.

Users of the Health Quest's wireless network must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise the Health Quest's information systems security.

Health Quest software, documentation, and all other types of internal information must not be sold or otherwise transferred to any party over the wireless network.

Internet cameras and personal wireless access points are strictly forbidden on the wireless network.

Additional Provisions By Subnet:

The wireless network is divided into three segments. One is intended for use by Health Quest-issued wireless devices, and will hereafter be called 'the wireless production subnet'. The second is intended for use by guests with their own wireless devices, and will hereafter be called 'the wireless guest subnet'. The last is intended for Health Quest doctors who bring in their own devices to use on the wireless network and will hereafter be called "the HQDoctor wireless network" The following additional provisions respectively apply to these network segments.

The Wireless Production Subnet:

No equipment that has not been issued by the Health Quest is permitted on the wireless production subnet.

Anyone using the Health Quest's wireless production subnet implicitly agrees to abide by the Health Quest's Breach of Confidentiality Policy, Confidential Information Policy, Internet Usage Policy, Protected Information Security and Confidentiality Agreement, and all other Health Quest, state and federal laws concerning appropriate use of technology resources, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

All packet data transmitted on the wireless production subnet is subject to monitoring by the Health Quest's Information Services Department. Inappropriate use of the wireless production subnet will be reported to the offending party's supervisor or manager and to the Chief Information Officer/Vice President of Information Services.

The Wireless Guest Subnet:

Health Quest's wireless guest subnet is a free service. Its principal intended audience is the Health Quest's patients and visitors, but limited and reasonable use of this subnet by Health Quest employees during their non-working hours, and by physicians, volunteers, consultants and/or contractors is also permitted. Emphasis in the foregoing sentence is upon the words "limited and reasonable." Users who are not patients or guests are not permitted to use the Health Quest's wireless guest subnet as a substitute for Internet service at their homes or offices.

The wireless guest subnet is not an intrinsic part of the Health Quest's business. Because of this, the Health Quest's Information Services Department will not assist users, regardless of their relationship with the Health Quest, with configuring their personal devices to access the wireless guest subnet. Users should be familiar with configuring their own equipment, and may contact their equipment manufacturer for assistance.

All use of the wireless guest subnet is at the user's own risk. Health Quest is not responsible if any user's personal information is compromised, or for any damage caused to a user's portable computer, device, or software while using the wireless guest subnet. Nor is Health Quest liable if any user's personal wireless device is lost or stolen.

As a public network, the wireless guest subnet is not inherently secure. Its users, and not Health Quest, are responsible for securing data transmission to and from their wireless devices, including but not limited to using encryption and personal firewalls and having up-to-date protection against viruses.

Under no circumstances should Health Quest business of any nature be conducted on the wireless guest subnet.

Although Health Quest provides the underlying network infrastructure of the wireless guest subnet, no transmission from it represents any position of Health Quest, and transmissions coming from the wireless guest subnet are not approved by Health Quest unless expressly stated therein. Users must not place Health Quest material on the wireless guest subnet.

Use of the wireless guest subnet by employees must not interfere with the employees' work.

Internet traffic on the wireless guest subnet is not filtered for content. Browsing the Internet over the wireless guest subnet may result in the user viewing content which he or she may find objectionable. Health Quest is not liable on this account.

Health Quest reserves the right to monitor, access, retrieve, read, and/or disclose communications through the wireless guest subnet when there is reasonable cause to suspect criminal activity or policy violation, or monitoring is required by law, regulation, or at the request of the Chief Information Officer/Sr. Vice-President of Information Services as appropriate under federal and state privacy laws and regulations.

All users of the wireless guest subnet explicitly and implicitly agree to hold Health Quest, its employees, agents, contractors and affiliates harmless from, and indemnify them against, any claim, liability, loss, damage, cost or expense, including attorney's fees, arising out of or related to their use of, or their inability to use, the wireless guest subnet.

The Wireless HQDoctor Subnet:

Physicians who bring their own personal devices to work for the purpose of accessing clinical applications can request that their equipment be connected to the HQDoctor wireless subnet. Their devices MAC address is added to a table which provides them access to this subnet. Benefits of this subnet for the provider is they no longer need to enter their email address upon connecting to the wireless network and greater bandwidth from guest wireless use.

Anyone using the Health Quest's wireless HQDoctor's subnet implicitly agrees to abide by the Health Quest's Breach of Confidentiality Policy, Confidential Information Policy, Internet Usage Policy, Protected Information Security and Confidentiality Agreement, and all other Health Quest, state and federal laws concerning appropriate use of technology resources, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

All packet data transmitted on the wireless HQDoctor subnet is subject to monitoring by the Health Quest's Information Services Department. Inappropriate use of the HQDoctor production subnet will be

reported to the offending party's supervisor or manager and to the Chief Information Officer/Vice President of Information Services.