

## **Medical Device Wireless Certification Process**

The number of medical devices on the Henry Ford Health System (HFHS) network has slowly increased over the last several years. This trend has been accelerated with the increased integration of IEEE 802.11 a/b/g/n wireless capabilities into medical devices.

Several large medical device manufacturers like Philips, GE, Medtronic, and Baxter are designing and manufacturing medical devices with ease of mobility and the unlicensed RF frequencies in mind. This document serves as a framework for testing medical devices to ensure that they are compatible with the standards based HFHS wireless network, and that they meet relevant regulatory standards.

The series of tests are tailored around type I, type II, and type III medical devices. These are defined as follows:

- Type I :** Non-Life sustaining devices which transmit or receive clinical data over the network which does not include ePHI<sup>i</sup> (electronic protected health information).
- Type II:** Non-Life sustaining devices which transmit or receive ePHI over the network
- Type III:** Life sustaining<sup>ii</sup> devices

Type I and II medical devices can be added to the HFHS wireless network if they support the necessary levels of authentication and encryption.

**Type III medical devices should not be added to the HFHS wireless network without written approval from HFHS CEO.** The unlicensed RF spectrum is susceptible to RF Jamming and other types of Dos attacks which could disrupt the functionality of these types of devices.

It is critical that every type of device introduced on to the HFHS wireless network be certified by Siemens IT personnel prior to being allowed on the network. A project request needs to be submitted for each desired certification. Most wireless devices require their wireless client to be optimized for a dense access point deployment like the one at HFHS.

The certification process entails the following:

- **Functional Testing**
- **Network Testing**
- **Failover and Redundancy Testing**

This document does not address the support mechanism / process for medical devices. This is addressed in a separate Operating Level Agreement (OLA) for the device.



## **Functional testing**

The first series of tests are intended to validate that the wireless medical device being evaluated is IEEE compliant. The following should be validated as part of the test:

- Is the wireless capable medical device designed to be mobile, or stationary?
- Does the device operate in the unlicensed RF Spectrum?
  - Is it IEEE 802.11a/b/g/n or any subset there-of compliant?
  - If not, what RF frequencies does it utilize?
  - Is it Wi-Fi certified?
  - What PHY rates are supported?
  - Is the wireless capability provided by a bolt-on bridge or an integrated wireless card?
  - What model of wireless card and chipset are used?
  - What is the average packet size transmitted, and the maximum latency and jitter requirement?
  - Does the wireless card on the device support "super frames"/frame aggregation (802.11n)?
- Is the device IEEE 802.11i compliant?
  - Is WPA2 encryption supported?
  - Does the device support 802.1X?
  - What types of EAP can the device support?
  - Can the device be added to a Windows domain within Active Directory?
- Is the device IEEE 802.11e compliant?
  - Does the device support WMM and/or WMM PS Mode?
  - What queue is recommended?
- Is the device IEEE 802.11r compliant?
  - Is fast secure roaming supported?
  - Is Opportunistic Key Caching supported?
- Can the device firmware be updated as wireless authentication and encryption mechanisms evolve in the industry?

## **Network test**

The series of tests/questions below are oriented towards understanding the impact of the proposed device on the wireless and the wired network.

- Does the device support DHCP, or does it require a static IP address?
- What type of information is transmitted via the wireless medium?
  - Is it required for the device to be on the corporate wireless network?
  - What does the device need access to on the corporate network. Can you list all appliances, and necessary TCP/UDP ports?
  - Does the device transmit ePHI (electronic protected health information)?
  - What is the network bandwidth requirement for the device?



---

**"Transforming lives and communities through health and wellness - one person at a time."**

- Can the MTU size be manually modified on the device if needed?
- Is the device HL7 compliant?

### **Failover and Redundancy test**

- In the event that there is a disruption to the wireless network, what actions are taken by the device?
  - Does it support/provide a backup mechanism for transmitting data if needed?
  - Does it automatically try to retransmit the data once network connectivity resumes?
  - Does it have a password protected administration mode for modifying network settings?
- If the device loses network connectivity, will it directly impact a life sustaining on-going process or procedure?
- Does the device support removable storage media?
  - Is USB or Firewire supported?
  - Does the device have an accessible/removable hard drive?
  - Does the device store ePHI (electronic protected health information) on removable media?

The medical device undergoing certification will be classified in the medical device certification report. All findings related to the questions posed above and additional observations will be addressed in the report



---

<sup>i</sup> ePHI (electronic protected health information) is data that contains any information that whether alone, or in conjunction with other information can help identify an individual/patient. Typical identifiers are:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city, county, or ZIP code)
- All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- FAX number
- Email address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Device identifiers or serial numbers
- Web URL
- IP address
- Finger or voice prints
- Photographic images
- Any other characteristic that could uniquely identify the individual

<sup>ii</sup> Life sustaining is used to define a medical device which relies on network connectivity in order to continue to provide necessary functionality for sustaining life. Loss of network connectivity directly impacts the ability of the device to perform functions necessary to sustain life.

