Johns Hopkins

Clinical Wireless Device Standards

Best Practices and Guidelines for Wireless Medical Devices, Clinical and Institutional System Integration, and Clinical Communications

Calvin Sproul

Approved by the ICSC, November 2011
Revisions Approved, May 2018

Table of Contents

I. Introduction 3

Purpose and Scope 4

Mobile Medical Applications (Apps) 5

II. Project Review 5

Network Wireless Support System Review 6

Client Technologies Solutions Support Approach 7

Clinical Engineering and Bio-Med Management Strategy (Patient Risk Assessment and Patient Safety FDA 510k) 7

Capital Finance, Compliance, and Legal System Review 8

Clinical Systems Review Committee 8

Security Authentication Encryption System Review 8

III. Project Phases 9

Proof of Concept 9

Pilot Candidate 9

Production Readiness 9

IV. Clinical Application Support 10

Interoperability, HL7 Interface and Location Awareness 10

System Server and Operational Support 10

V. Attachment A 11

Mobile Device/Smart Phone Security 11

VI. Attachment B 12

Preparation and Implementation Work Plan 12

VII. Attachment C 13

VOIP QoS Questionnaire 13

VIII. Attachment D 15

Wireless Medical Device Pre-Survey Questionnaire 15

IX. Attachment E 17

VoWi-Fi, WLC, and Cisco Recommendations and Requirements 17

X. Attachment F 19

QoS Settings for VOIP on Wireless Controller per vendor 19

XI. Attachment G 20

Device Certification 20

XII. Attachment H 22

Device Compatibility 22

XII. Appendix A 23

Personal Communication Device 23

Introduction

An increasing number of medical devices now have wireless Ethernet capabilities. They are presently in the Johns Hopkins' clinical environment. These devices collect patient health information and send it back to database servers. The patient health data transmits through the wireless interfaces to the clinical applications and server databases. There is a concern by hospitals and health centers about medical device attaching to the wireless network and protecting patient health information according to privacy laws. The Food and Drug Administration (FDA)[1] responded to the concern by releasing a Medical Device Data System (MDDS) proposal in 2008. The proposal asked medical device and equipment manufacturers to come up with standards and best practices on deploying medical devices in a clinical environment. The resulting standards are ISO/IEC 80001-1:2010. [2]

The challenge and opportunity with clinical wireless medical devices is to determine if a single purpose modality will work in combination with other various clinical devices. This trend to combine functionality is already evident with messaging and voice devices. With combined functions, we can gain efficiencies using fewer devices. Messages sent by medical alert and alarms systems are going to devices that were traditionally voice only. The combination of bar code scanning and printer could provide similar efficiencies. It will greatly simplify connectivity, administration and monitoring.

Securing the wireless device connection is a concern. WEP (Wired Equivalent Privacy) is a flawed encryption method and no new wireless devices will connect to the Clinical Wireless network using this method. Enterprise WPA2 (Wi-Fi Protected Access), EAP[3] (Extensible Authentication Protocol), SHA-2[4] (Secure Hash Algorithm) and AES[5] (Advanced Encryption Standard), must be used to secure the wireless device.

Wireless devices must follow the most current wireless standards. A walk around survey will demonstrate whether the new devices will co-exist with established devices. There are finite limits on the number of wireless devices that can connect in a given area. The potential for over-subscription is of primary concern. Vendor recommended configuration settings for some devices often conflict with the recommended configuration for other vendor devices. This situation can easily cause interference and disruption to one or both systems or devices. Listed are examples of Clinical Wireless Devices currently on the network.

[1] http://www.fda.gov/MedicalDevices/default.htm

[2] Request for Document ISO/IEC 80001-1:2010 can be made at the International Organization for Standards website http://www.iso.org/iso/home.htm

[3] http://www.rfc-archive.org/getrfc.php?rfc=4017

[4] https://csrc.nist.gov/csrc/media/publications/fips/180/4/final/documents/fips180-4-draft-aug2014.pdf

[5] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

Clinical Wireless Devices

Care Fusion Motorola MC75a scanners and Zebra QL220 label printers
Masimo Vital Signs monitors (pilot)
Honeywell Refrigeration Temperature monitoring
Zoll Defibrillators
Ascom phones in support of GE Nurse Call
Nova Glucose-Meter Medical/lab devices and Aegis Point of Care
GE Portable X-ray machines (Radiology has model name list)
Portable Ultra-Sound (same as Portable X-Ray)
Alaris IV Pumps
GE QS Fetal Monitoring
Vioptix Pulse Oximeter

In a related development, the clinical environment is seeing the increased use of mobile devices and phones like the Smartphone. Apple's *iPhone* and the Google *Droid* are two common examples that are becoming more popular and powerful. These devices have PC-like capabilities with substantial and easy to install applications. For example, these applications can look at physiological monitor waveforms and report back vital signs to staff and clinicians. If clinical wireless device is involved in patient care, it is a medical device. Go to "Mobile Device/Smart Phone Security" policy to reference securing these types of devices. Included is an excerpt from the applicable best practices policy in Attachment A. Go to Attachment H for a table of the latest supported wireless devices used in the Clinical Environment.

Purpose and Scope

The purpose of the Clinical Wireless Device Standards is to support the development and deployment of clinical technologies:

1) Ensure the safe and effective use of clinical wireless devices at Johns Hopkins.

2) Ensure that other wireless devices do not interfere with the safe and effective use of clinical wireless devices at Johns Hopkins.

3) Encourage innovation in the use of clinical wireless technology.

4) Address issues of usability, security, device management, systems integration and consistency with technology trends.

These Standards cover hardware, device operating systems, and pilot medical devices. General-purpose COTS (Commercial off the Shelf) wireless devices such as Androids, iPhones, iPads and PCDs (Personal Communication Devices refer to Appendix A) and covered at a high level. Applications (e.g. Apps) that may be included on such devices, including browser-based or HTML5 applications may not apply under this standard yet covered under Hopkins policies and procedures such as ICSC standards and the CSRC process discussed below. The boundary between application and device may not always be clear, however, and it may be appropriate to seek guidance according to the links and contacts below. This document is an accompaniment to Johns Hopkins Hospital and Health System policy. Hospital policy will supersede any policy outlined in this document if there is a contradiction between the two.

Mobile Medical Applications (Apps)

The FDA is currently working on regulatory guidance named, "Draft Guidance for Industry and Food and Drug Administration Staff Mobile Medical Application". Its intended purpose is to "apply its regulatory requirements solely on a subset of mobile apps that is calling mobile medical applications or "mobile medical apps."". "Software applications that run on a desktop computer, laptop computer, remotely on a website or "cloud," or on a handheld computer may be subject to device regulation if they are intended for use in the diagnosis or the cure, mitigation, treatment, or prevention of disease or to affected structure or any function of the body of man." The "Mobile Medical App" that displays, stores, or transmits patient specific medical data constitutes an MDDS (Medical Device Data System) links to the clinical wireless device on which it runs and come under review by the appropriate policy committee. In this case, the Clinical Data and Documentation Committee (CDDC) would review the considered clinical wireless medical device. [6]

II. Project Review

This section details the clinical medical device review before the new device's introduction into the Clinical Wireless Environment. The following is a quick checklist to perform before determining the device can enter into the project phases (section IV).

- **No WEP (Wired Equivalent Protection). Unsecure and not suitable for clinical environment.**
- **No Multicast. It connects one device to many devices. Will cause network issues.**
- **Must use 256 bit AES (Advanced Encryption Security). The encryption referenced in HIPAA/HITECH.**
- **Must use Management software. This is the only realistic way to update devices remotely.**
- **Must survey for wireless signal strength in the clinical environment where it is used.**
- **Must certify and validate wireless device in the clinical environment.**
- **Must be able to remote wipe device where PHI (Patient Health Information) is stored.**
- **Must use 802.11g[7] or 802.11a[8] standards. It is advisable to use 5 GHz frequency and 802.11n standards.**
- **No bridges or single purpose SSID (Service Set Identification) network.**
- **Must register all wireless device MAC addresses with Enterprise DHCP.**
- **It is advisable to authenticate devices that interface with restricted systems.**

[6] http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

[7] http://standards.ieee.org/getieee802/download/802.11g-2003.pdf

[8] http://standards.ieee.org/getieee802/download/802.11a-1999.pdf

Network Wireless Support System Review

Project evaluation commences with the **Project Application System Support Document and Template**. Reference the Johns Hopkins Standards web site[9] for the template. This is critical information for any clinical application project. Refer to Attachment B for a work-plan task list in preparation for vendor engagement. Medical Device vendors typically have a prepared network questionnaire to determine if the host environment is prepared to connect the medical device and support system to the network. The appropriate Johns Hopkins clinical department or review committee answer the questions, sends the completed questionnaire back the vendor. This is a preliminary step provides an opportunity to address basic issues, and concerns in the network environment.

When the vendor questionnaire is complete, the Johns Hopkins Network team sends a questionnaire to the vendor to complete. The appropriate questionnaires are included in this document as attachments. Refer to Attachment C if there is integrated Voice and Messaging Service necessary for a system such as Nurse Call. Refer to Attachment D if the device is data only. The filled out network questionnaire is sent back to the Johns Hopkins Network team for further review.

After the Johns Hopkins Clinical Wireless Questionnaire returns from the vendor, a network analysis of the wireless controllers takes place to ensure that the wireless configuration is properly set to the vendor best practices. The vendor outlines the technical settings in their documentation. If the wireless controller settings need to change from default settings, impact testing will need to take place against wireless devices already on the production network.

When the initial wireless network analysis is complete, the appropriate support group becomes involved. The designated support group test various administrative and support features in a pilot environment. After confirmation of the device configuration, a comprehensive management strategy and planned implementation approach is developed.

Device support groups at the Johns Hopkins Hospital are:

- Client Technologies Solutions (CTS) - They have extensive expertise with client devices like smart phones and wireless laptops.
- Clinical Engineering/Bio-Med – They provide support for the primary modality of medical devices at Johns Hopkins with or without wireless connectivity.
- Telecommunication Support – They support voice handsets through the Private Branch Exchange (PBX) and network using Voice over Internet Protocol.

Voice over Internet Protocol (VOIP) using wireless networks and Quality of Service (QoS) needs special consideration. Consequently, this will affect the number of access points in a given area and tagged packets to prioritize the delivery of voice over wireless. Refer to Attachment E and Attachment F for special settings with wireless phones used in Clinical Nurse Call systems.

An **important strategic requirement** moving forward in the New Clinical Building is the use of the **5GHz radio**. There is less interference and more channel bandwidth in this unlicensed

[9] http://www.it.johnshopkins.edu/policies/standards.html

frequency than in the very crowded 2.4 GHz. It is imperative for clinical systems to utilize 5GHz frequency instead of the lower 2.4GHz.

Client Technologies Solutions Support Approach

Support of Clinical Medical devices once they are in the hospital normally belong to either the Client Technologies Solutions (formerly known as Desktop Computing Services), or the Information Technology group that directly supports the department using the equipment. A recent example is handheld bar code scanners and printers used by Pathology Lab Data Systems using wireless data connectivity.

Finding the right remote administration and monitoring application for Clinical Medical Devices under consideration for deployment in the hospital is a prime concern and is essential to the success of any medical device deployment. Remote administration can deploy firmware code updates, remote data wipes, and perform troubleshooting. Client Technologies Solutions has broad experience with data devices and remote support applications in the hospital using administrative monitoring programs.

Clinical Engineering and Bio-Med Management Strategy

(Patient Risk Assessment and Patient Safety FDA 510k[10])

The Johns Hopkins Clinical Engineering/Bio-Med staff has traditionally been the first contact when purchasing new medical devices by clinical departments at Johns Hopkins. It is essential for Clinical Engineering/Bio-Med to have an opportunity to evaluate the considered medical device and ensure it adheres to FDA 510k Patient Risk Assessment regulations.

When clinical employees use a wireless medical device next to a patient, we must be positive the device will do no harm. There are microwave signals emitted from the new generation of wireless medical devices. These devices have the potential to cause interference with other devices in proximity to the patient. Patients' bodies may block certain microwave signals. If the medical device is depending on having a reliable wireless connection, this blockage may be an issue, and is especially an issue if the device is sending alerts and alarms to pagers.

Bench testing by Clinical Engineering using standard testing methodology is a typical way to determine patient risk when wireless devices are under consideration. In all cases, Clinical Engineering staff will need to review and test the medical device according to best practices and standards. Clinical Engineering staff must work with Clinical Application staff to determine application, server, and hardware requirements including the following:

- Server – Minimum memory and CPU, staging, interface feeds, backup, failover, virtualization, database size requirements. Designate System Administrator.
- Data Storage – Determine Interaction with existing Clinical Applications, Client connectivity, Data Storage size, and licensing.
- Workflow - Testing with Clinical Staff, confirm connectivity where it will be needed, forecast numbers of devices connected to system when fully deployed and readiness of infrastructure for full capacity.

[10] **Section 510(k)** of the Federal Food, Drug, and Cosmetic Act requires those device manufacturers who must register to notify FDA, at least 90 days in advance, of their intent to market a medical device. Source www.fda.gov.

- Wireless device must be capable of 802.11n standards and have the capability for both 2.4GHz/5GHz radio frequencies.

Capital Finance, Compliance, and Legal System Review

The Capital Planning Group will need notification when considering new medical systems that involve patient care, and the procurement groups need notification so they can compare the systems to other systems in the hospital and determine if bulk purchases can reduce unit costs.

Capital and Finance can assist in the development of a Request for Information (RFI) and a Request for Proposal (RFP). The structure of the RFP is to account for product price considerations and make recommendations for the best feature set in the market place. The Purchasing group may also interact with Legal to write conditions into contracts we execute with various vendors to ensure protection for both Johns Hopkins and the vendors.

Clinical Systems Review Committee

All systems that affect patient care must fill out a Patient and Security risk assessment form. The Clinical Systems Review Committee (CSRC) provides the form. The implementer of the project, usually the assigned Project Manager, outlines risk factors pertaining to the implementation and deployment of the project. The CSRC reviews the completed form and considers the indicated medical devices and systems that have patient contact. These systems need to adhere to regulatory criteria and interact with other clinical applications used to treat and examine patients. The CSRC takes a critical look at project, security and risk management. The patient risk assessment is a requirement by HIPAA.

The Clinical Data and Documentation Committee (CDDC) is a related clinical review committee to the CSRC. The CDDC focuses on data collected by clinical applications and ensures that standard clinical system interfaces (for example, HL7, ADT, EMR, etc...) adheres to best practices. The CDDC determines whether patient health information is secure and properly integrated into existing clinical systems. How the data are stored, secured, and backed up in a database program such as SQL is another important area reviewed by the committee.

A good reference on the subject of Health Care Risk Management is “Aiming for Patient Safety in a Health Care Environment”[11]. This document by Todd Cooper and Sherman Eagle describes how various Health Care Standards Committees, such as Association for the Advancement of Medical Instrumentation (AAMI), influenced the development of ISO 80001-1:2010 standards pertaining to medical devices.

Security Authentication Encryption System Review

Recent HIPAA/HITECH regulations came out declaring that Wired Equivalent Privacy (WEP) may no longer carry Patient Health Information (PHI) for clinical wireless systems and applications. The encryption and authentication must be Enterprise WPA2 (Wi-Fi Protected Access) Enterprise authentication, SHA-2 (Secure Hash Algorithm), and Advanced Encryption

[11] “Aiming for Patient Safety in a Health Care Environment” by Cooper/Eagle http://www.aami.org/publications/ITHorizons/2010/18-20_StandardsRegs_Cooper.pdf

Standard (AES) compliant. This regulation provides protection to the network and the patient care devices. Johns Hopkins Wireless offers two types of WPA encryption:

- “Hopkins” Service Set Identifier (SSID) has Protected Extensible Authentication Protocol (PEAP), Microsoft Challenge Handshake Protocol (MSCHAPv2), AES and userid/password from the Johns Hopkins Enterprise Directory (JHED) to create hash values and encrypt a session.

- “JHAccess” SSID has Extensible Authentication Protocol- Transport Layer Security (EAP-TLS) using the Johns Hopkins Certificate Authority which is integrated into the Johns Hopkins Active Directory domain using Public/Private Key exchange.

III. Project Phases

Proof of Concept

As a general matter concerning project management, it is best practice to incorporate a “Proof of Concept” phase into any project testing. Use it to determine the effectiveness of the device and application, whether it interferes with other medical devices, and if it actually works as advertised and documented. Only on-site testing can determine whether basic functionality works, not marketing brochures. The resulting analysis can establish true benefits and shortcomings. It is best to resolve any issues or shortcomings before the device deployment in a clinical environment. Testing and comparisons between medical device competitors take place during this phase of the project. The JHOC Simulation Center has proved valuable as a place to do proof of concept deployments.

Pilot Candidate

After the Proof of Concept is completed and we establish the system is safe for the clinical environment, the pilot phase can begin. Pilots take place in a very limited clinical environment. We can test the full functionality in a demonstrative proof of concept tested with clinical workflow. Sponsorship for the pilots include the stakeholder’s described in the planning documentation. The various clinical departments, which sponsor new wireless clinical devices, have a stake in the new medical device and application implementation to ensure they work reliably. The Pilot Phase is the appropriate phase to contact Facilities Project Management if infrastructure is necessary to support the pilot. The infrastructure could include data wiring or power to support data connectivity and collection. The assigned Facility Project Manager is will create an Installation Project Plan. The Project Manager will coordinate the efforts of the vendor according to their specifications**.**

Production Readiness

When considering new wireless system deployments at the hospital, there is a determination on whether the new deployment will co-exist with other wireless devices in the environment. Surveys in the areas of deployment are essential to check for coverage, capacity, roaming, and keeping a consistent reliable network connection. Other considerations may be special needs surrounding Quality of Service (QoS), or impact on workflow when used by staff.

Multicasting is a requirement on some patient vital sign monitoring systems. Traditionally, systems that require a multicasting segment are separate from production networks and work in their own closed network environment. Integration of formally closed networks through gateways will be necessary to accept transmission of patient vital sign data.

Workflow training for battery life and charger maintenance must take place. Documentation, such as writing dates onto batteries when they go into production, can help verify when batteries replacement is necessary.

At the end of the Production Readiness phase is a process called "Device Certification." Originally created for Computers on Wheels, the process outline is in Attachment G and is a useful template.

IV. Clinical Application Support

Interoperability, HL7 Interface and Location Awareness

Medical Devices commonly interact with other clinical applications such as Admission Discharge Transfer (ADT), Provider Order Entry (POE), BDM Pharmacy, and Electronic Medical Record (EMR). These systems interact though an interface such HL7 or Nightingale reviewed by the CRSC. Information processed through wireless devices may update an EMR patient record, or provide drug interaction information to a drug formulary database. Interface data can provide alert and alarm information to a Nurse Call system or even location awareness and status if needed in an emergency. There is potential to locate or track devices leading to a reduction of equipment purchases. Quick access to equipment location information is essential for clinical staff when tracking down life-saving medical equipment.

System Server and Operational Support

Application Data Support systems that come with the medical devices include SQL databases and server support. Database size determines the decisions concerning the capacity and availability of server and information storage. Medical Devices such as IV pumps have back-end support services that guard against delivering improper drugs and dosages. Technical considerations for the server environment include, Content Switching, High Availability, and Disaster Recovery. The Enterprise Services server group is equipped to install a server running virtualization and apply best practices following healthcare industry standards.

V. Attachment A

Mobile Device/Smart Phone Security

7. Mobile Device/Smart Phone Security

Policy 6 in the original, complete document addresses the physical security of mobile devices, including the statement, “Confidential information may not be stored on portable devices or other media unless encrypted.” Security for handheld devices, many of which serve as telephones and text message communicators, has several unique characteristics:

a. Use enterprise-supported devices where possible to ensure appropriate security settings.

b. When setting up, access Hopkins directly (e.g. through JH Exchange or JHEM) so as to take advantage of Hopkins system functionality and minimize the likelihood that messages or user credentials will be intercepted or stored by a third party carrier or service. (Please note Policy that requires users to avoid disclosing credentials to administrators, including device setup and maintenance.)

c. Choose a strong password or pin. The security of your system is only as strong as the password. It may be difficult to type especially complex passwords on the small keypad of some devices, but it is important to create the strongest reasonable passwords.

d. Minimize data exposure by limiting the number of messages stored by the mobile device. In some cases, this requires users or administrators to change default device settings.

e. Email and address books, while not Restricted information, should be considered sensitive and worth protection.

f. Keep current with OS and security updates. As threats emerge, it may become necessary to install additional security, including anti-virus, anti-spyware and/or intrusion detection.

g. Verify encryption mechanisms for data at rest (where restricted information is likely to be stored) and transmissions. Do not permit transmission of user accounts and/or passwords over the wireless networks. Johns Hopkins Secure Connect VPN provides encryption for many device types.

h. Use remote “kill” functionality where possible. These allow users or administrators to delete data from a lost or stolen device rapidly.

i. Promptly report lost or stolen devices.

j. Reduce security risk by limiting your device to only necessary applications and services. Unnecessary applications may create security and usability issues and drain device bandwidth and battery life. Bluetooth and IR are two examples of services that can open devices to unwelcome access if improperly configured.

k. Follow safe disposal practices by removing all sensitive information first. Enterprise-supported devices will generally back this up.

VI. Attachment B

Preparation and Implementation Work Plan

Task Assignment	Task
Enterprise Network Wireless, Device Support, Clinical Engineering, and Telecommunications	Work with Vendor to determine if coverage and capacity is sufficient in the environment. Test wireless devices and simulate workflow.
Enterprise Services and Clinical Application Support	Setup test server and interfaces with proposed vendor devices to ensure they connect properly with expected results. Ensure other clinical systems (i.e. ADT) get data through standard interfaces.
Enterprise Network Services	Test special considerations such as content switching or load balancing. Ensure other clinical systems can get data through interfaces.
Department Customer and Enterprise Directory Services	Sponsor JHED credentials for vendor. This is for remote access into the piloted systems. Vendors can update test systems remotely and make quick adjustments or updates.
Enterprise Network and Enterprise Network Security	Ensure correct port access or gateway access configuration for the piloted system. Test access when new clinical devices are in pre-production employment along with new services.
Device Support and Client Technologies Solutions Support	Ensure best practices software like anti-virus protection, patch management or backup procedures do not impede or block data flow from devices to the server or various other clinical system interfaces.
Departmental Customer and Clinical Application Project Management	Ensure the development of proper training for clinical staff so they can effectively work with the new system.
Clinical Application Project Management	Ensure vendor implementation documentation matches Johns Hopkins Project Implementation Plan.

VII. Attachment C

VOIP QoS Questionnaire

1. **VPN (Virtual Private Network) provided through Johns Hopkins sponsorship for remote access. Is it necessary?**

2. **A "Guest" wireless network provided on the shared wireless network access points at Johns Hopkins. Do you foresee issues with this?**

3. **Does the device need QoS (Quality of Service) to perform properly?**

4. **If answer is yes to the above question then:**
   What 802.1p priority values do you require? (i.e. 6?) What DSCP value will you require on the LAN switch? (i.e. 46?)

5. **Is it necessary to broadcast the SSID (Service Set Identifier)?**

6. **What kind of authentication method can you use? Open, WPA-PSK (Pre-Shared Key), WPA2-PSK, PEAP-MSCHAPv2, EAP-TLS?**

7. **What kind of encryption can you use? WEP (Wired Equivalent Privacy), TKIP (Temporal Key Interval), AES (Advanced Encryption Security) CCMP (**Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)**?**

8. **What vendor's wireless infrastructure do you recommend? (E.g. Cisco, Aruba, Meru, Trapeze, Meraki, etc…)**

9. **What level of network infrastructure firmware do you recommend? List by vendors indicated above.**

10. **Does your system include a gateway? Any other translation or support services? Will it need a static ip address or will a manually registered dynamic ip address suffice?**

11. **What protocols does the device support? (H.323, G711, SIP)**

12. **Will you need a Johns Hopkins site NTP (Network Time Protocol) server?**

13. **Will the device need WMM (Wi-Fi Multi-Media) IEEE 802.11e Wireless QoS configuration?**

14. **Will the device deploy U-APSD (Unscheduled – Automatic Power Saving Delivery) and PS (Power Save) - Polling?**

15. **Do you use SIP (Session Initiation Protocol) and SIP trunking? Do we need to increase the SIP server license? Can the path to the SIP server pass through a firewall?**

16. **Do you know the number of devices for the project? (Estimated for capacity purposes). Do you know how devices can simultaneously connect to single access points?**

17. **What is the expected SNR (Signal to Noise Ratio) and signal level when handing off and roaming between adjacent access points?**

VIII. Attachment D

Wireless Medical Device Pre-Survey Questionnaire

Vendor: ____

Manufacturer: ____

Contact Name: ____

Address: ____

E-Mail: ____

1. Does the Wi-Fi adaptor / device support 5 GHz frequency? Yes/No

2. Does the Wi-Fi adaptor / device support Enterprise WPA-2 (Wireless Protected Access)? Yes/No

    AES (Advanced Encryption Standard) with Enterprise Authentication? Yes/No

    EAP-TLS (Extensible Authentication Protocol/Transport Layer Security)? Yes/No

3. Does the Wi-Fi adaptor / device support SHA-2 (256 bit) certificates for network authentication? Yes/No

4. Does the Wi-Fi adaptor / device support 802.11r (Fast Transition for 802.1x)? Yes/No

5. Does the Wi-Fi adaptor / device support 802.11k (Neighbor List)? Yes/No

6. Does the Wi-Fi adaptor / device support 802.11v (Transition Control Management)? Yes/No

7. Any restrictions on DFS (Dynamic Frequency Selection) or 802.11h channel announcements? Yes/No

8. Any restrictions with channel bonding? Yes/No

9. Any restrictions with DHCP (Dynamic Host Control Protocol)? Yes/No

10. Any restrictions with DDNS (Dynamic Domain Naming Service)? Yes/No

11. Does the device require static IP address? Yes/No

12. Any restrictions for using hidden SSID’s (Service Set Identification/No Broadcast)? Yes/No

13. Does your device support the updated Regulatory Domain ‘B’ for the USA (Channels and adjusted power settings)? Yes/No

14. Does your device support IPv6 (Internet Protocol version 6)? Yes/No

15. Can your device be set to a specific frequency band (2.4GHz or 5GHz)? Yes/No

16. Is the wireless adapter 802.11ac capable? Yes/No

17. Does the medical device need its own router to connect to the wireless network infrastructure?

Additional Questions:

18. Do you have a technical data specification for your handset/ devices with a recommended configurations guide for the wireless controller (Cisco)? If so, please attach.

____

____

____

19. Any known interoperability bugs or issues with Johns Hopkins production Cisco WLC (Wireless LAN Controller) code (at present 8.3.133.0 MR3 subject to change)?

____

____

____

____

20. Any Advanced WLAN Configuration settings recommended (i.e. Such as DTIM)?

____

____

____

____

21. Does your medical device/app have an interoperability guide? If so, please attach.

____

____

____

____

22. Do you have a central management solution to manage the configurations?

____

____

____

____

23. Will your devices work with any MDM (Mobile Device Manager) solutions (i.e. Air Watch, In Tune)?

____

____

____

24. What is the recommended RSSI (Receive Signal Strength Indicator) for your device to roam between Wireless Access Points?
____
____
____
______

25. What are the QoS (Quality of Service/WMM/802.11e) requirements if any?
____
____
____

IX. Attachment E

VoWi-Fi, WLC, and Cisco Recommendations and Requirements

Radio Settings

- All of the following have a global configuration on the Cisco 4400 WLC for QoS Quality of Service.
- Enable "Aironet IE" to let the Ascom VoWi-Fi handset make use of CCX for enhanced configuration.

Performance on VOIP WLAN

- Use only channels 1, 6 and 11, which are the only 2.4GHz, channels non-interfering globally on all campuses.
  (Caveat) Do not enable RF grouping or Dynamic Channel Assignment since these settings will create an inconsistent radio environment.

- Avoid dynamic transmission power by settings Tx Power Level Assignment to Fixed **(Caveat)** this will affect all wireless access points on a global scale and may create problems for POE clients. The default settings will work fine but to optimize the recommendation is to disallow 802.11b clients to associate by setting the (6) Megabits rate to mandatory in the 802.11g configuration.

- It is also highly recommended to disable all lower 802.11b speeds in the Cisco WLC infrastructure to obtain even higher performance:

  a. **Transmission rate 1, 2, 5.5 should be disabled**
  b. **Transmission rate 6 should be set as mandatory**
  c. **Other rates should be set as supported**

Beacon Period

The default beacon period is 100 ms and is the recommendation. However, if there are access points of model 1252 in the system, the beacon period should be set to 102 ms since the 1252 APs cannot use a 100 ms period.

Unscheduled – Automatic Power Saving and Delivery (U-APSD)

When using U-APSD in the handset, it is very important that the WMM parameters in the Cisco WLC are set correctly, since U-APSD handles a bi-directional data stream where the uplink and downlink transmit within the same Enhanced Distributed Channel Access (EDCA) Category.

To use U-APSD, make sure to set QoS to "Platinum" for the current WLAN profile and set WMM to "Allowed." Set EDCA profile for 802.11b/g to "Voice Optimized" and enable low latency MAC.

- This will prioritize all wireless traffic to voice on a global scale.
- Test with other QoS devices when introduced to the environment.
- Disable Session Timeout for the current WLAN profile to avoid reoccurring de-authentications.
- It is also highly recommended to disable Broadcast Forwarding since this will avoid unnecessary traffic on the WLAN used for voice.

Call Capacity

If voice power save mode "Active" is used, the Cisco WLC infrastructure can handle up to **31 calls per AP**. If voice power save mode "**U-APSD" is used, it can handle up to 35 calls** per AP because packets buffer at the access point. This applies if no data traffic is present and no channel re-use is necessary.

Depending on the data traffic load, cell coverage and co-channel interference, resulting in a capacity reduction around 10 calls per AP. If using 802.11bg (instead of a pure 802.11g system) the call capacity may decrease even more.

Handover Performance

The handover performance is heavily dependent on the chosen security scheme. The authentication process, as well as the exchange of fresh session encryption keys, affects the time needed to perform an inter-BSS transition before the transmission of and resumption of speech frames.

The list below shows an average of handover times with different security settings. The stated times are a guide and assistance in the choice of security scheme and not displayed as absolute numbers. A number of factors such as external Remote Access Dial-in User Service (RADIUS) server performance, channel usage etc… will affect the handover time.

Authentication scheme/Encryption type ~ Handover time

- Open NONE ~ 11 ms
- Open WEP ~ 12 ms

- WPA-PSK TKIP ~ 35 ms
- WPA2-PSK AES-CCMP ~ 28 ms
- LEAP (Lightweight Extensible Access Protocol) WEP ~ 37 ms
- LEAP TKIP ~ 45 ms
- LEAP with CCKM TKIP ~ 12 ms
- PEAP-MSCHAPv2 with opportunistic key caching
- AES-CCMP ~ 30 ms

X. Attachment F

QoS Settings for VOIP on Wireless Controller per vendor

(Deprecated, present requirements are for 5Ghz. Vendor configuration take precedent)

Controller configuration guidelines

Cisco 79xx phones:

1. Set "Quality of Service (QoS)" to "Platinum"
2. Set the "WMM Policy" is set to "Allowed" or "Required"
3. Enable "Aironet IE"
4. Disable "P2P (Peer to Peer) Blocking Action" / "Public Secure Packet Forwarding (PSPF)"
5. Disable "DHCP Address Assignment"
6. Set "MFP Client Protection" to disabled or optional
7. Enable "Admission Control Mandatory" for Voice
8. Enable "Load Based CAC (Cisco Call Control)" for Voice
9. Disable "Admission Control Mandatory" for Video
10. Set "EDCA Profile" to "Voice Optimized"
11. Disable "Enable Low Latency MAC"
12. Disable "Aggressive Load Balancing" is disabled
13. Enable "Symmetric Mobile Tunneling Mode" when using Layer 3 mobility
14. Disable "ARP (Address Resolution Protocol) Unicast" where proxy ARP will be enabled
15. Enable "DTPC" (Dynamic Transmit Power Control)
16. Enable "Short Preamble" if using 2.4 GHz

ASCOM i75 phone requirements

Controller configuration guidelines

1. Prefer New VLAN (Virtual Local Area Network) for ASCOM Voice only.
2. WMM Policy set to "Required" affects present Vocera deployment, which uses dated 802.11b standards.
3. QoS Profile 802.1p, 802.1p tag 6
4. DTIM = 5 when not using U-APSD (Uninterrupted-Automatic Power Saving and Delivery), Cisco default is 1 DTIM (Delivery Time Interval Message).

5. Beacon Period for ASCOM i75 and Cisco 1252 access point = 102 (100 for all others)
6. Custom set 802.11b/g/n 2.4 GHz radio. Set RF Channel assignment to custom. Set TX Power Level Assignment to custom.
7. WLAN (Wireless Local Area Network) edit 802.11g only, which affects Vocera 802.11b.
8. Do not use 7920 AP CAC or Client CAC for ASCOM.
9. Disable "Enable Session Timeout".
10. Call Admission Control (CAC), TSPEC (Traffic Specification). ASCOM recommends not turning on. Disable radio for TSPEC configuration.
11. TSPEC Max RF Bandwidth 75% and Reserve Roaming Bandwidth 6%.
12. EDCA Parameters. Disable Radio for EDCA. Profile Voice Optimized and Enable Low Latency. Cisco recommends disable Low Latency.
13. ASCOM VOIP Gateway interface must be set with VLAN and priority.

Care Fusion

Custom Commands CLI (Command Line Interface)

1. config advanced 802.11b channel dca sensitivity high
2. config advanced 802.11b tx-power-control-thres -75
3. config advanced 802.11a tx-power-control-thresh <-50 to -80>
4. config advanced 802.11b tx-power-control-thresh <-50 to -80>

XI. Attachment G

Device Certification

This attachment addresses specifics of doing a wireless Workstation on Wheels (WOW) certification. This procedure supports the Clinical Documentation and Provider Order Entry (POE) application on Public WOWs. Extension and modifications to this procedure may be necessary to fit various Clinical Applications/Devices concerning patient care. If the certified environment, the changes need to be reviewed and the devices re-certified.

The checklist below outlines the collection data for analysis. The Application Support group can then make decision on whether the environment can be "certified." If the test does not meet the above criteria, the remediation area undergoes retesting to satisfy the certification requirements.

Checklist:

- Open a browser window to the wireless access controller, which is controlling the access points in the test environment. Open the client monitor to ensure the Media Access Control (MAC) addresses of the WOWs can connect to the closest proximity access point. Ensure that as the WOW moves around the floor, it roams to the nearest access point.

- Confirm that the WOW is connecting 802.11a (5 GHz) and not “flapping” to 802.11g (2.4 GHz).

- Check the access point in the controller and make sure the configuration is for the right AP group and subnet interface.

- Go to client monitor and make sure the WOW is picking up the right IP address for the area. Sometimes, the WOW configuration is from the lab and retains the IP address from the lab environment. Correct the ip address by removing the client from within the client monitor on the controller and renewing the DHCP address on the client.

- Define and confirm the area where the WOWs are moving around. Ensure the signal is uniformly “excellent.”

- Record the IP addresses, MAC addresses, and firmware driver levels of the wireless access points and the WOWs.

- Is the wireless adapter on the WOW 802.11a (5 GHz) capable and set to 802.11a only?

- Is Windows Zero Configuration used? Is it a proper driver installed?

- Access Points consist of a minimum standard Cisco enterprise standard model 3500, 3600, and 3700 with 802.11ac. Swap out access Points and upgrade in the clinical area if not the standard model.

- Is there robust signal coverage on the Critical Care Unit with properly staggered channels so there is no co-channel interference?

- Do an extended ping test on the device at the command line to ensure no packet latency greater than 200 milliseconds. Travel around the Critical Care unit in a typical rounding pattern or into patient rooms to simulate clinical staff workflow.

- Test the Provider Order Entry or the appropriate Clinical Application. Open the clinical application on the device and make sure that the application does not close during rounding. The closing of the application requires a userid/password to resume and loss of screen information. Of course, this is a tremendous inconvenience to clinical staff performing patient care.

- Follow WOW testing on the Wireless Controllers. Ensure that it is roaming properly from access point to access point and is connecting at maximum data speed.

As hardware goes through refresh cycles, replace and fix devices. Upgrade drivers and configuration changes made to clinical devices. Do the certification process at regular intervals on the units. Examination of the electrical outlets should be a part of the certification and done on a regular basis on all the Clinical units. Power management has been an issue with battery management stations, the plugs in the wall, and the power in data closets. Poor battery performance will sometimes manifest itself with slow data connection speeds.

XII. Attachment H

Device Compatibility

Manufacture	*Model*	*Works*	*OS Version (Min)*	*OS*
Zebra	MC40	Yes	4.4.4 Android	Kitkat
	SB1	Yes	Latest Firmware	Windows CE
	MC55	No	N/A	Windows CE
	MC65	No	N/A	N/A
	MC75	No	N/A	N/A
	MC70	No	N/A	N/A
	QLn220HC	Yes	Latest Firmware	N/A
	QLn320HC	Yes	Latest Firmware	N/A
	QLn220	Yes	Latest Firmware	N/A
	QLn320	Yes	Latest Firmware	N/A
Android (Phones)	S3 / S3 Edge	Maybe	4.0.4	Ice cream
	S4 / S4 Edge	Maybe	4.2.2	Jellybean
	S5 / S5 Edge	Maybe	4.4.2	Kitkat
	S6 / S6 Edge	YES	5.0.2	Lollipop
	S7 / S7 Edge	YES	6	Marshmallow
	S8 / S8 Edge	YES	7	Nougat
	Core	YES	5.1.1	Lollipop
	Note 4	Maybe	4.4	Kitkat
	Note 3	Maybe	4.2.2	Jellybean
	Note 2	Maybe	4.0.4	Ice cream
	Nexus 4	Maybe	4	Ice cream
	Nexus 5	Maybe	4.4.0	Kitkat
	Nexus 6	YES	5	Lollipop
	Nexus 7	Maybe	4.3	Jellybean
Honeywell	CT50	Yes	6.0 Android	Marshmallow
Samsung	Tab S2	Yes	6.0 Android	Marshmallow
	Tab S3	Yes	6.0 Android	Marshmallow

Microsoft	Surface	Yes	Firmware date: 08/24/2017	Windows 10
Apple	Macbook	Yes	10.13 High Sierra	MacOS
	Macbook Air	Yes	10.13 High Sierra	MacOS
	Macbook Pro	Yes	10.13 High Sierra	MacOS
	Ipad	Yes	11	IOS
	Ipad Mini	Yes	11	IOS
	Ipad Pro	Yes	11	IOS
	Iphone 6S	Yes	11	IOS
	Iphone 7	Yes	11	IOS
	Iphone 8	Yes	11	IOS
	Iphone X	Yes	11	IOS
Google	Chromebook	Yes	Latest Updates	ChromeOS
Dell	Laptops	Yes	Latest updates from WNIC Manufacture.	

XII. Appendix A

Personal Communication Device

Personal Communication Devices, better known as PCS, not covered in this document.

Johns Hopkins Human Resource Policy HR613 defines them below.

Personal Communication Devices – Electronic media or communication devices like, but not limited to, cell phones, pagers, text pagers, wireless devices, etc.[12]

[12] http://www.hopkinsmedicine.org/jhhr/policiesprocedures/HR613_10.1.08.DOC