The Center for Medical Interoperability
Operational Requirements & Guidelines

Trusted Wireless Health

CMI-ORG-TWH-D01-20180913

Draft

Notice

This Operational Requirements & Guidelines document is the result of a cooperative effort undertaken at the direction of The Center for Medical Interoperability for the benefit of The Center's members and its customers. You may download, copy, distribute, and reference the documents herein only for the purpose of developing products or services in accordance with such documents, and educational use. Except as granted by The Center in a separate written license agreement, no license is granted to modify the documents herein (except via the Engineering Change process), or to use, copy, modify or distribute the documents for any other purpose.

This document may contain references to other documents not owned or controlled by The Center. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document. To the extent this document contains or refers to documents of third parties, you agree to abide by the terms of any licenses associated with such third-party documents, including open source licenses, if any.

© 2018 Center for Medical Interoperability (The Center)

DISCLAIMER

This document is furnished on an "AS IS" basis and neither The Center nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and The Center and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

The Center reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by The Center or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from The Center, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	CMI-ORG-TWH-D01-20180913			
Document Title:	Trusted Wireless Health			
Revision History:	D01 – 09/13/2018			
Date:	September 13, 2018			
Status:	~~Work in progress~~	**Draft**	~~Released~~	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~The Center /Member~~	~~**The Center/ Member/ NDA Vendor**~~	Public

Contents

1 INTRODUCTION

1.1 Introduction and Purpose

This document presents Trusted Wireless Health (TWH), a set of proposed requirements and guidelines for Health Delivery Organizations (HDOs) to develop and maintain wireless infrastructure that is consistent, responsive, and secure. This approach makes connectivity a commodity, building a foundation for interoperability at higher levels of the Open Systems Interconnection (OSI) model. Compliance with the operational requirements in this document enables HDOs to provide a foundation for interoperability.

1.2 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are listed below and are as defined by [IETF RFC 2119]:

“SHALL”	This word means that the item is an absolute requirement of this specification.
“SHALL NOT”	This phrase means that the item is an absolute prohibition of this specification.
“SHOULD”	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
“SHOULD NOT”	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
“MAY”	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 REFERENCES

2.1 Normative References

This document does not use normative references.

2.2 Informative References

[IETF RFC 2119]	"Key words for use in RFCs to Indicate Requirement Level", https://tools.ietf.org/html/rfc2119
[802.11a]	IEEE 802.11a-1999: Telecommunications and Information Exchange Between Systems — LAN/MAN Specific Requirements — Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band, 2003.
[802.11ac	IEEE 802.11ac-Enhancement for 802.11n, 2013
[802.11b]	IEEE 802.11b-1999: Telecommunications and information exchange between systems — Local and Metropolitan networks — Specific requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band, 2003.
[802.11e]	IEEE 802.11e: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, 2005.
[802.11g]	IEEE 802.11g: Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band, 2003.
[802.11n]	IEEE 802.11n: Enhancement for higher throughput, 2009.
[802.11r]	IEEE 802.11r: Amendment for fast BSS Transitions, 2008.
[802.11ac]	IEEE 802.11ac Enhancement for higher throughput 2013
Wi-Fi Vantage™2.0	Wi-Fi® Alliance Vantage 2.0, 2016
[WFA Hotspot 2.0]	Wi-Fi® Alliance: Hotspot 2.0 Release 2, 2014.
[WFA WPA2™]	Wi-Fi® Alliance: Wi-Fi® Protected Access (WPA) Enhanced Security Implementation Based on IEEE P802.11i standard, Version 3.1, August, 2004.

2.3 Reference Acquisition

- Center for Medical Interoperability (The Center), 8 City Boulevard, Suite 203 | Nashville, TN 37209, USA; Phone +1-615-257-6410; https://medicalinteroperability.org/
- Wi-Fi® Alliance (WFA), 10900-B Stonelake Boulevard, Suite 126, Austin, Texas 78759 USA; Phone: +1 512 498 9434; https://www.wi-fi.org/

3 TERMS AND DEFINITIONS

This document uses the following terms:

Clinical Network	Directly pertaining to care delivery, including technical, financial, or communication tasks
Cell	Intended area of service for a wireless access point
DMARK	Demarcation point where a carrier equipment transitions to a local administration equipment
Enterprise Network	Companion tasks to care delivery, including technical, financial, or communication tasks on non-public network
Guest Network	Unrelated to care delivery, originates from patients or visitors

4 ABBREVIATIONS AND ACRONYMS

This document uses the following abbreviations:

AAA	Authentication, Authorization, and Accounting
AP	Access Point
BYOD	Bring your own device
CLI	Command Line Interface
CMI	Center for Medical Interoperability
dBm	Decibels relative to one milliwatt (mW)
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized zone (external facing network)
DHCP	Dynamic Host Configuration Protocol
EIRP	Equivalent Isotropic Radiated Power
FTT	Flexible Time Triggered
GHz	Gigahertz
HDO	Healthcare Delivery Organization
IDF	Intermediate distribution frame
IP	Internet protocol
Mbp/s	Megabits per second
MDF	Main distribution frame
MCS	Modulation and Coding Scheme
NSD	Network Services Devices
NTP	Network Time Protocol
OSI	Open Systems Interconnection
PoE	Power over ethernet
RF	Radio Frequency
RRM	Radio Resource Management
SNR	Signal to noise ratio
SSID	Service Set Identifier
TWH	Trusted Wireless Health
VLAN	Virtual local area network

VoIP	Voice over IP
WFA	WiFi Alliance
WLC	Wireless LAN Controller

5 TRUSTED WIRELESS HEALTH (TWH) INFRASTRUCTURE REQUIREMENTS

This Section presents Trusted Wireless Health requirements related to the wireless infrastructure, specifically wireless Access Point (AP) deployment, configuration and security.

5.1 AP Deployment

APs SHALL be configured such that Clinical Network traffic is not impeded by competing traffic. This can be accomplished by carrying guest traffic and enterprise traffic on different radios and on different channels. By separating these networks, the large and growing volume of patient care and clinical care personnel traffic is isolated from guest traffic, thus freeing up airtime and bandwidth for enterprise and clinical applications. One way guest traffic separation MAY be accomplished is by placing all guest traffic on the 2.4 GHz band, leaving the 5 GHz band for enterprise and clinical communication.

The availability of wireless signal is critical to rapid and error-free transmission of health data. APs SHALL be located to ensure a minimum signal level of -63 dBm, for each SSID, and will be available in 99.5% of the covered area as measured in an RF survey using 100 square feet sampling grids. This survey is performed in the use environment of the network, after construction is complete, to ensure the measured signal levels reflect conditions during care. Similar wireless surveys and traffic monitoring, discussed in Appendix I.4, will be performed at regular intervals to inform necessary changes as the installation ages. The noise floor SHALL be at or below -87dBm in the ISM 2.4 GHz and 5 GHz bands, as measured during the wireless survey.. These signal levels, and the resultant 24dB minimum SNR, are aligned to achieve on average 36 Mb/s data transmission at a Packet Error Rate (PER) of 2%.

A regular grid of APs provides dense coverage while minimizing interference with neighboring APs. APs SHALL be separated by a minimum of 50dB of attenuation/path loss to avoid near-field interference, as measured by no AP receiving a signal from its neighbor at a level of -42dBm or greater. As a rule of thumb, this can be achieved by placing APs no closer than 12' (3.5m) to the next nearest AP. APs operating on the same channel SHALL be separated by a minimum of 82dB of attenuation. This will often equate to placing each AP an average of 44' (13.5m), plus or minus 2' (0.6m), from its nearest neighbor operating on the same channel.

It is critical that all APs operating on the same wireless channel are separated by enough distance and dense material that none impedes any other's clear channel assessments. In order to provide the proper coverage for 2.4 GHz, the power would be reduced, or some of the APs (about ½) would be disabled from transmitting, or a combination of the two.

To avoid interference from overlapping channels, each layer of wireless traffic SHOULD use six or fewer unique channels with a minimum separation of 20MHz between center frequencies. APs serving overlapping Cells SHALL NOT use the same channel. Interference can be limited by placing APs out of their neighbor's line of sight and by ensuring APs on the same channel have at least one Cell of separation.

The environment immediately surrounding an AP can have an outsize effect on performance, and so care must be taken to avoid environmental interference. AP antenna elements SHOULD be placed below the ceiling. APs SHOULD be placed away from obstructions such as I-beams. To ensure coverage in elevators, which are mobile and fully enclosed, APs SHOULD be mounted in elevator cars and attenuated to -30dB., although local building codes will need to be adhered to. Additionally, each AP SHOULD be mounted in a tamper resistant box below a ground plane of 2' x 2' (6 to 8 inches surrounding AP), or larger, although antenna manufactures documentation SHOULD be consulted to insure optimal configuration.

5.2 AP Configuration

Each AP SHALL be configured to transmit at +8 dBm EIRP, plus or minus 3dBM to accommodate local structural circumstances.. This promotes symmetric communication with wireless devices and permits a smaller Cell size, thus increasing the capacity of the network. Wireless LAN Controllers (WLCs) SHALL be configured so that automated RF systems (e.g. RRM) run no more frequently than once per day and run at a low usage time. APs SHALL disable [802.11b].. APs serving Enterprise Networks or Clinical Networks SHALL support 5Ghz [802.11n] wireless.

All APs SHALL support Wi-Fi Alliance Vantage 2.0™ including the optional FTT/r/fast session transfer, which enables prioritization and efficient client roaming behavior with supported devices. APs serving the Enterprise clinical network SHALL support [WFA Hotspot 2.0] to aid with discovery and mutually authenticated secure wireless access.

APs SHALL be configured with a beacon data rate of either 12 Mbp/s or 24 Mbp/s. For all APs, data rates for [802.11a]/[802.11g] SHOULD include 6, 12, 24, & 36 Mbp/s and exclude 9, 18, 48, and 54 Mbp/s. For all APs, Modulation and Coding Scheme (MCS) data rates (802.11n/802.11ac) SHOULD be enabled.

Multicast SHOULD be disabled or minimized on all APs.

APs SHOULD NOT be configured with hidden SSIDs, as any hidden SSID will cause devices to probe. WLCs SHOULD be configured so no more than three SSIDs are offered in any one band (2.4 GHz/5 GHz) to maximize performance.

5.3 AP Security

APs SHALL authenticate and encrypt all wireless enterprise network communications. APs SHALL require EAP-TLS authentication, or equivalent, (e.g. EAP-SIM on enterprise networks and clinical networks. All devices operating on these networks will be individually credentialed in order to support secure, revocable, and auditable access.

Wireless access controllers SHALL be configured to use 802.1X authentication on ports with physical outlets outside the Main Distribution Frame or Intermediate Distribution Frame (MDF/IDF). Unauthenticated equipment SHALL be disallowed on enterprise networks.

Appendix I Operational Guidelines

This section presents common items useful for the design and implementation of a robust wireless network. These are presented as an informative addendum for network engineers.

I.1 MDF/IDF

Physical and logical network diagrams will be current and readily available. Wired Network components (routers, switches, firewalls, etc.), hereafter referred to as Network Services Devices (NSDs) will be located in the MDF / IDF spaces. MDF / IDF spaces may be co-located with non-network (data transmission) equipment (e.g. servers) and general Information Technology (IT) equipment. An MDF/IDF space will not be co-located with materials that have no direct connection with network or server type equipment (e.g. custodial closet).

An MDF/IDF will be sized to properly rack and cable all core servers and core network gear, as well as the connection DMARK services. Racks in the MDF/IDF are better positioned with at least 3.3'(1m) distance in front and behind for equipment and wiring access.

Switches in the MDF will ideally be under the control of one supervisor engine configured for high reliability and redundancy. IDF to MDF links will be redundant and distributed equally across the IDF switches. IDFs supporting wireless AP connections will have a minimum of three switches configured in a stack. APs will ideally be connected across multiple switches so that the complete failure of a switch will affect fewer than a third of APs on a given floor in any area. Since APs are commonly physically located in a triangular array, with vertices A, B, and C – each vertex can be connected to a different IDF switch.

To solve problems of infection control, aesthetics, RF ground plane needs, and radio placement physics, APs should ideally be mounted in a cut-out in a recessed ceiling cabinet.

The MDF/IDF will ideally be fire resistant as to ingress or egress of a fire and will be equipped with an electronics safe fire suppression system. The MDF/IDF power source will ideally allow for generator backup. The MDF/IDF backup power source will ideally be configured to condition power and sized to support 1-2 hours at 75% processing capacity of a fully populated rack. The MDF/IDF power supply will ideally alert administrative personnel on battery use status when operating on battery power. Cooling in the MDF/IDF will ideally be 125% of expected offered BTUs from all equipment. NSDs providing power-over-Ethernet (PoE) will have redundant power supplies so that failure of one power supply does not take down any APs. Temperature in the MDF/IDF will ideally be no higher than 68 degrees F (20 degrees C).

The MDF/IDF will ideally have a remote, recorded, time-stamped camera which provides a record of activity. The entrance to the MDF/IDF will ideally be locked with restricted access with mechanical key or electronic key-card access.

I.2 Routing

A redundant firewall will be configured with multiple defined virtual networks (VLANs): external (carrier circuit), guest, DMZ, and private – ordered from most public-facing to most private-facing. The private network may be further divided behind the firewall into functional areas such as, but not limited to, business office, database servers, enterprise services, clinical services, biomed engineering, medical devices, and nurse call or phone systems. In turn these networks could be divided into OSI Layer 3 routable traffic to limit broadcast traffic in the network and unintended consequences to small areas.

Network equipment will have an IP address on a private management VLAN, to restrict remote access. It is recommended to select a management VLAN, other than the default management VLAN (usually named VLAN1)…

Guest traffic will only have access to the carrier public internet.

To connect devices which do not support authentication (e.g. printers), fixed VLAN ports could be placed on the firewall in a network located between the private and the DMZ security levels.

DHCP Servers will ideally be configured to preserve IP address space used by NSDs for routing purposes. Link-state routing protocols will ideally be implemented over any form of distance vector protocols. NSDs will point to a redundant Network Time Protocol (NTP) server.

Each HDO may provision Wi-Fi® calling routes and access list filters for VoIP systems to balance reliability of calls made over Wi-Fi®.

I.3 Security

All AAA access activity logs will be preserved for a specified period (e.g., three years). NSDs will use secure connections, including Command Line Interface (CLI) access. NSD's will use AAA for all management access.

I.4 Traffic Monitoring

Traffic loads on the network will be assessed periodically (e.g., twice or more per year). The HDO will regularly scan for unauthorized access and work to eliminate their connection to networks.

Stationary devices (e.g. printers) will not be on the wireless network, and will have local wireless disabled.

BYOD devices will have a mobile device management system (MDM) to monitor compliance to ensure compliance to established uses and responsibilities.

Guest traffic access will ideally be changed periodically (e.g., monthly) to reduce traffic from unexpected sources (e.g., neighboring businesses).

Multicast packets will ideally be converted to unicast, and IGMP configured to distribute traffic only to APs with interested clients.

VoIP traffic will ideally be on an SSID that addresses the impact of roam-time on signal quality. For enterprise or clinical VoIP traffic, [802.11r] protocols can help ensure fast, secure roaming. The HDO will ideally use content filters for traffic monitoring.

Appendix II Acknowledgements

The Center and its member companies would like to extend a heartfelt thanks to all those who participated in the development of this document.

Mitchell A. Ross was the primary author of this document. **Bowen Shaner** was the primary editor.

Bernie McKibben, Chris Riha, Sumanth Channabasappa, Trevor Pavey and Ed Miller provided review comments. **Katy Hoyer** served as the document editor. **Jessie Hanson** provided review**.**

The following individuals supplied valued comments during the review process, Kai Hassing, George Cragg, Brent Bonner, Mark Weary