CHANGE HISTORY			
Change Date:	**Rev**	**Description of Change:**	**By:**
Unknown	001	Initial Release	Unknown
Unknown	002 - 004	Unknown	Unknown
10/24/2012	005	Unknown	R. Evans
12/26/2013	006	Unknown	R. Evans M. Ghodoussi G. Brallier
5/5/2014	007	Updated sections, & with Whitepaper	K. Temby
4/7/2015	008	Updated name and branding references	K. Temby
04/28/2015	009	Updated sections 3.3 (Encryption) and 3.5 (Provider Access User Authentication).	Walt Villalba
3/7/2016	010	Separated out Viewpoint & Class I section	K. Temby
09/14/2018	011	Bandwidth revision, AD revision, wireless revision	K. Trimboli
3/18/2020	012	Changes, which were not tracked, were simple edits for readability and to make the document shorter. Also, I removed the text box on page 6, changed revision number, shortened the document from 10 pages to 8 and added section 1.8 Updates by Andy, Bill, and Cheryl. Updates to companion document, MB-15513-026: If your company uses e-mail filtering software (i.e. spam, junk), we request whitelisting the "@TeladocHealth.com" and "@visitnow.org" e-mail domains and our dedicated sending IPs: 13.111.63.220 and 69.72.41.191. This will ensure your teams receive our timely operational notifications for required maintenance, emergency product outages, and quarterly release notes	C. Kelmar A. Young, B. Stout
12/4/2020	013	Changed format and branding to match Teladoc Health guidelines	L. Jaitman
12/22/2021	014	Updating terminology Medical Devices to Telemedicine Devices, updating Imaging section	L. Jaitman J. Mears

Table of Contents

1 Unauthorized Hardware or Software Changes to Teladoc Health Telemedicine Devices....3
2 Purpose and Scope....4
3 Best Practices: Patient Access Telemedicine Devices on Hospital Networks....4
3.1 Remote Presence Network and System....4
3.2 Software on Patient Access Devices....4
3.3 Operating System....4
3.4 Patches and Updates....5
3.5 Software on Teladoc Health Viewpoint....5
3.6 Network Settings for User Authentication of Teladoc Health Patient Access Devices....5
3.7 Active Directory Domain Membership....6
3.8 Supported Wireless Network Types....6
Teladoc Health Technical Support....6
4 Teladoc Health Telehealth Network....6
4.1 Basic Operation....6
4.2 Firewall Requirements....7
4.3 Proxy Configurations....7
4.4 Wireless Access Point (WAP) coverage and Site Evaluation....7
4.5 Wireless Technology....7
4.6 Bandwidth Requirements....7
4.7 Network Priority and Quality of Service (QOS)....8
4.8 Connectivity Requirements....8
4.9 Satellite-based Remote Presence Networks....9
5 IT Specifications for Patient Access....9
5.1 Patient Access Systems....9
5.2 Encoding Information....9
5.3 Encryption....9
5.4 Virus Protection....10
5.5 Provider Access User Authentication....10
5.6 Teladoc Health Imaging Installation....10

1 Unauthorized Hardware or Software Changes to Teladoc Health Telemedicine Devices

The Teladoc Health Telemedicine System is a complex, state-of-the-art telemedicine device containing hardware and software components. Unauthorized changes to any of these components can do harm to the device. All Teladoc Health Telemedicine System Reference Manuals include the following warning statement:

"Adding third party software or hardware to the Telemedicine System may cause it to malfunction or operate erratically. Teladoc Health does not support the addition of third-party software or hardware to a remote presence end point".

Examples of unauthorized changes to an Teladoc Health Patient Access Device include but are not limited to:

- Addition, revision or removal of hardware components.
- Addition, revision or removal of software applications.
- Changes/updates to existing installed software drivers.
- Changes to the Windows Operating System. Teladoc Health manages this remotely and validates changes.

The Teladoc Health Telemedicine System is a mission-critical telemedicine device and the configuration must be maintained as required by Teladoc Health. Network requirements for optimal Telemedicine System operation are documented separately in MB-15513 Network Configuration for Teladoc Health Devices.

2 Purpose and Scope

This document contains required information to guide local IT in network configuration to ensure a successful telemedicine program. It should be provided prior to installation to allow adequate time for implementation.

3 Best Practices: Patient Access Telemedicine Devices on Hospital Networks

3.1 Telemedicine Network and System

Teladoc Health Patient Access Devices are telemedicine devices that are intended to be continuously connected to the Teladoc Health Telehealth Network. The Teladoc Health Telehealth Network should be considered mission critical in the overall safety and treatment of the patients, as well as the daily operation of remote physicians.

Teladoc Health Telemedicine System provides physicians with remote access to the hospital from their home, office or hospital. It is comprised of the Provider Access Software Apps, including iPad, iPhone, or Windows computer; Hardware Patient Access Device, including Teladoc Health Vita, Teladoc Health Lite, Teladoc Health Vantage and Teladoc Health Xpress, Teladoc Health Vici, Teladoc Health TV, Teladoc Health TV Pro; or Software Patient Access device, which is Viewpoint-Installed on Hospital provided Windows machine or iPad. The Provider Access and Patient Access Devices are linked via the Internet over a secure connection. All Patient Access Devices can operate on an 802.11 Wi-Fi network and Ethernet.

3.2 Software on Patient Access Devices

Patient Access Devices must NOT be managed the same as the Enterprise File Server or a generic Workstations. Enterprise-wide Microsoft Windows Policies pushed out over the Network to all Workstations should NOT be pushed to any Telemedicine Device or mission critical system. No third-party software installed throughout the enterprise network on typical servers and Workstations may be installed on any of the mission critical Patient Access Devices.

The Teladoc Health telemedicine device software is classified as a component of the telemedicine device. Software that has not been validated by the manufacturer (Teladoc Health) must not be installed. **The uses of any software other than those specified will violate the safety, effectiveness, and design of the telemedicine device. Such use may result in an increased risk to users and patients**

3.3 Operating System

Teladoc Health Patient Access Devices run on Microsoft Windows platforms and Linux within some subsystems. Each Teladoc Health software application has passed quality assurance verification with a version and configuration of the Windows Operating System. The configuration of the tested Windows Operating System and Teladoc Health software shall not

be altered in any way since this may invalidate the pre-defined environment of the telemedicine device.

3.4 Patches and Updates

Teladoc Health manages the latest qualified Operating Systems for use with their hardware devices. Updates are formally controlled via Teladoc Health Preventive Maintenance and OS verification testing in the appropriate environment.

3.5 Software on Teladoc Health Viewpoint

Teladoc Health Viewpoint Patient Access system is a software solution installed on hospital owned, Windows based computer/tablet or Apple iPad, and should not be managed the same as a customer's Enterprise File Server or PC Kiosk. Teladoc Health Viewpoint should ONLY receive Anti-Virus software and updates as other Hospital Network Servers and Workstations. Domain policies, such as powering down systems or changing login rules will negatively impact the functionality of Viewpoint software. Teladoc Health does not provide onsite support for their Viewpoint software patient access solution.

3.6 Network Settings for User Authentication of Teladoc Health Patient Access Devices

Teladoc Health's Patient Access Devices require an un-obstructed path to the URLs, IP addresses, Ports, and Protocols described in MB-15513. Devices should be isolated from discovery of other devices and resources on the hospital network. Installation and testing instructions are in SP-20026 Wireless Network Connection Guidelines for Teladoc Patient Access Devices. The most common issues affecting Patient Access Devices are Proxy Devices, Intrusion Detection System (IDS), Web or Content filtering devices, and inadequate bandwidth. The Patient Access and Provider access devices/applications do not require access to customer servers or resources to function. They only require a secure network connection to access the internet. In order of highest preference first, the following network configurations are supported:

Reliability	IP Assignment	Wi-Fi Access	QOS	Routing
Best	Static IP address	Dedicated SSID or VLAN with PSK Authentication for all mobile devices.	VOIP QOS settings	Static route around all packet inspection devices. 1to1 NAT of external/internal IP to ensure optimal connectivity. Isolating the device within a DMZ is highly recommended
Good	DHCP (Static sometimes required)	Existing VOIP SSID (or other SSID with QOS)	VOIP QOS settings	Static route around packet inspection devices
Minimum	DHCP (Static sometimes required)	Existing telemedicine device SSID	Ability to set QOS by device	Static route around packet inspection devices

3.7 Active Directory Domain Membership

Active directory Domain Membership is not supported on any Teladoc Health Patient Access Device, except for Viewpoint software installations.

3.8 Supported Wireless Network Types

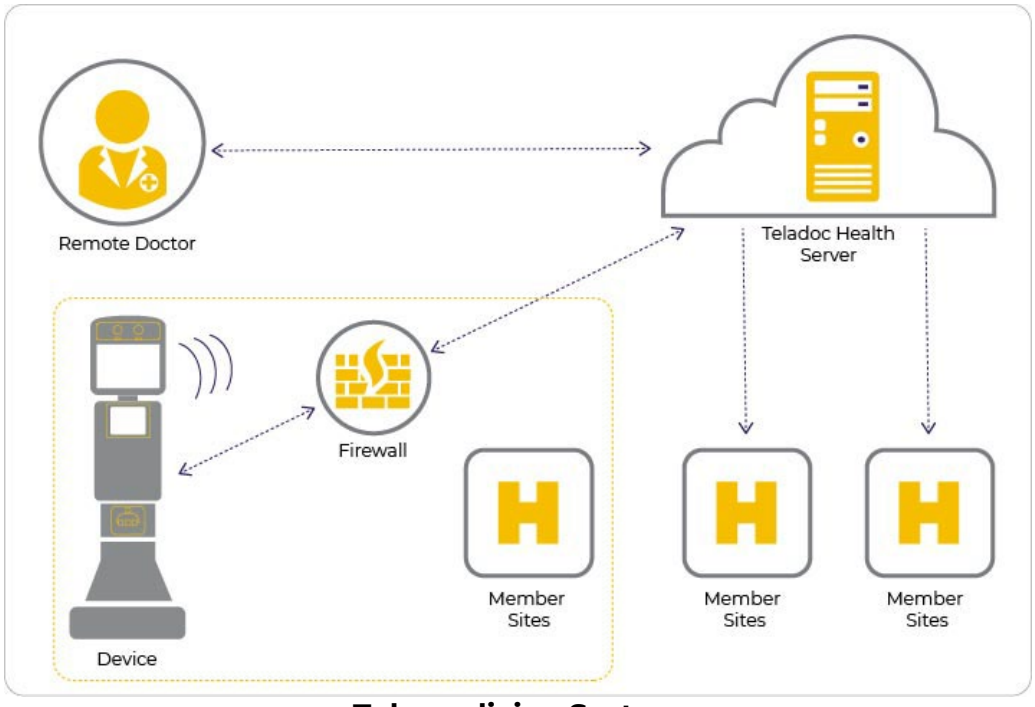
Guest, Staff, VIP, or other non-clinical SSID's are not suitable for connection of a clinical use endpoint for patient care. Teladoc Health Telemedicine devices must be connected to a managed clinical network for optimal performance.

Teladoc Health Technical Support
24/7 Live Phone Support
877-484-9119
805-562-8686 (select option 2 when prompted)
TAC@TeladocHealth.com

4 Teladoc Health Telehealth Network

4.1 Basic Operation

Teladoc Health maintains two parallel connectivity paths in our client and server software; a proprietary communication protocol and a standards-based SIP solution. Teladoc Health Patient and Provider Access software use these protocols to transmit control, video, and audio data. The Teladoc Health Network is a collection of integrated server infrastructure components that are located in network data centers across the world. The basic operation of both systems are outlined in the diagram below.



Telemedicine System

4.2 Firewall Requirements

For a list of IP addresses and ports to white list, refer to MB-15513 Network Configuration for Teladoc Health Devices. Additional modifications may be necessary for use with a Web Filter and/or Stateful Packet Inspection.

The protocol includes Transport Layer Security (TLS) Session Initiation Protocol (SIP) signaling communication on TCP ports 443, 5061 & 8100 with UDP communication on ports 35000-45000. The Interactive Connectivity Establishment (ICE) algorithm is used by Teladoc Health SIP Clients for Network Address Translation (NAT) conforming to RFC 5245. The Media Relay Server within the Teladoc Health SIP Server Package utilizes Session Traversal Utilities for NAT (STUN) and Traversal Using Relays for NAT (TURN). The TURN Server behavior conforms to RFC 5389, RFC 5766.

The Teladoc Health Network logs usage and error information. All devices behind firewalls require outgoing HTTP and HTTPS access (outgoing TCP through port 443) at a minimum. For training and support purposes (including software upgrades), Teladoc Health requires access to all Patient Access devices via Kaseya, a secure remote desktop application.

4.3 Proxy Configurations

Proxy routing/forwarder servers are supported. The Proxy Server IP address and port must be configured on the Patient Access device at the application level under the supervision of a Product Specialist. Third-party proxy clients and Operating System level proxy settings operating through Winsock or otherwise are not supported.

4.4 Wireless Access Point (WAP) coverage and Site Evaluation

It is essential to ensure coverage of WAPs is enough for the operational area of the Patient Access device. We recommend the hospital network administrator use a network that is not heavily used by other devices on a channel that does not have interference from other WAP's. This can be evaluated using a Network Profiling tool with the assistance of an expert Teladoc Health Product Specialist during a full site evaluation.

4.5 Wireless Technology

Teladoc Health Patient Access devices are compatible with 802.11a/g/ng protocols at a minimum and AC in later models. The Maximum Handoff Threshold time must be less than 150ms. Patient Access devices are required to smoothly transition between Wireless Access Points (WAPs). WAP Roaming must be supported by hospital network. Roaming can also be tested during installation and site evaluation.

4.6 Bandwidth Requirements

The telemedicine system device can be configured to utilize up to 4000kbps to provide the highest quality audio and video stream. The system can function with as little as 300kbps. Optimal bandwidth must be determined based on the available bandwidth, use case, and

Device Type. Use of Peripheral devices, i.e. Stethoscope, Otoscope, etc., will increase minimum bandwidth requirements.

4.7 Network Priority and Quality of Service (QOS)

Patient and Provider Access devices require QOS or IP traffic priority to ensure a connection under standard best practices. The QOS should guarantee that network traffic will traverse from the device out of the hospital and return from the internet to the Device at the optimum identified bandwidth. Issues in environments that experience network congestion, WAP coverage, and Wi-Fi congestion that are usually a bottleneck must be addressed first.

4.8 Connectivity Requirements

Network performance is critical to a responsive session. Therefore, metrics cover a range of network characteristics that impact the delivery of IP data packets in the proper order and timely fashion. Teladoc Health runs tests using proprietary third-party software tools to ensure that the broadband connection (wired or wireless) meets the standards for network performance to maintain a session. We can provide recommendations for these tools to customers upon request.

Due to the variability of the Internet during any session, quality may be degraded, or the session may be disconnected if the network performance limits described below are not met. This sometimes occurs even though performance measurements met minimum specifications at another point in time. There are five important network characteristics affecting connectivity, shown in Table 1: Network Performance Specifications.

Name	Spec	Description
Data rate	≥ 300kbps, ≥ 4000kbps (ideal)	A connection must have the required up-stream and downstream bandwidth
Latency	≤ 300ms	Max average network latency (delay) on a connection
Packet Loss	≤ 3%	Max connection packet loss
Jitter	≤ +/- 50ms	Jitter is variability in latency. Spec should not be exceeded during 95% of the duration of a session.
MTU	≥ 1400 bytes	The Maximum Transfer Unit must not be set below the spec

Table 1: Network Performance Specifications

Teladoc Health software dynamically adjusts for normal variability of data over the Internet. Performance of the hospital network's internet access must be tested. Failure to meet network requirements is a customer network malfunction.

4.9 Satellite-based Remote Presence Networks

Minimum network performance detailed above is required to achieve an audio/video session over a satellite network, except for latency typical of satellite networks. Teladoc Health's Telehealth Network can maintain quality sessions with latency up to 900 ms if all other network characteristics are met. Such a delay will be evident on both sides of any audio, video, or command communication, as is typical of satellite networks. When using a satellite network with latency above 600 ms, the delay in drive commands may hinder the operator from maintaining safe control over the movement of mobile Patient Access devices. Therefore, we do not recommend using mobile devices, such as the Teladoc Health Vita, on a satellite network where the minimum QoS parameters cannot be maintained.

5 IT Specifications for Patient Access

5.1 Patient Access Systems

Teladoc Health Patient Access is based on a mobile, robotic communications platform that enables a physician to have remote access to the hospital from their home, office or within the hospital. The Teladoc Health Telemedicine System is comprised of the Provider Access (Windows, iPad, iPhone) and Patient Access device (Teladoc Health Vita, Lite, Vantage, Mini, Viewpoint, or Xpress) communicating through the internet using the secure Teladoc Health Telehealth Network. All Patient Access devices operate on an 802.11 Wi-Fi network and support wired Ethernet. The telemedicine System communicates with the Teladoc Health Clinical Integration Tools and Teladoc Health Imaging platform for access to patient documentation and radiology imaging.

5.2 Encoding Information

Video is captured at 30 frames per second but can be reduced for low bandwidth connections. The Teladoc Health dynamic bandwidth algorithm provides the ability to dynamically adjust resolution and video quality during a live session without user interaction. Advanced users can specify preferences for adjusting resolution. Video quality depends on factors such as Patient Access Device motion, available bandwidth, and user preference.
Teladoc Health uses the ITU-T H.264 standard codec for video and the Opus and Speex codecs for audio.

5.3 Encryption

Our Proprietary Protocol (SharedComm) uses both asymmetric and symmetric cryptography. All systems communicate with our servers over a channel secured with TLS when performing operations such as user authentication and authorization (connectivity permissions). When a session begins, a random AES-256 symmetric key is generated and exchanged between the parties using RSA-4096 public-key cryptography. A new symmetric key is generated for each session and used to secure the session data, including audio and video.

The Teladoc Health SIP Protocol uses secure authentication and streaming via the TLS protocol. AES-256 encryption is used in all SIP signaling operations, including user authentication and authorization. Media encryption in SIP sessions is done with AES-256. The network is not accessible to SIP clients that are not part of the Teladoc Health Telehealth Network.

5.4 Virus Protection

TrendMicro's OfficeScan® is installed on every Hardware Patient Access system. This software automatically updates when new virus definitions are available. Teladoc Health staff installs all security updates on these devices. If the customer's IT department elects to manage the Provider Access and Teladoc Health Viewpoint security policies, our IT and Technical Services should be consulted prior to doing so, as updates may conflict with the correct operation.

5.5 Provider Access User Authentication

The Provider Access Application requires user authentication on startup. Strong passwords are required. Integration with customer Active directory is available to allow the provider to use their local domain username and password. Additional information on integration is available in MB-20100 Enterprise authentication documentation. When integration is not configured, we manage all user accounts and passwords. It is recommended that Windows passwords be employed to protect the system from potential damage by unauthorized users.

If the Provider Access Application is not connected to a Patient Access Device and is inactive (i.e., no mouse or keyboard input) it will automatically log out the user and close as a means of protecting the system from unauthorized access. The inactivity timeout can be configured to 5, 15 or 30 minutes.

5.6 Teladoc Health Imaging Installation

The Teladoc Health Imaging platform consists of a server, offered either as a physical gateway or virtualized, with an application configured to connect to the hospital Medical Imaging Management and Processing System or MIMPS (previously called "PACS") or radiology modalities. It connects to the Teladoc Health Telehealth Network so remote physicians may access and view the Radiology scans. See MA-20019 Teladoc Health Imaging Module Implementation Guide and MB-20249 Network Configuration for Teladoc Health Imaging Platform. An overview follows:

Networking Configuration Requirements

1. Three static "internal" IP addresses. Only one is needed for the virtualized platform.
2. Three static "public" IP addresses, unless using a VPN-type configuration.
3. NAT rules to route from the Teladoc Health hosted data centers to the location's public IPs, then to the internal IPs using certain ports.
4. If placed in a DMZ, internal routes are also needed each way between the Teladoc Health Imaging portal to/from the MIMPS on assigned ports.
5. If VPN, configuration is pre-determined to use available addresses and routing.

6. Any routes to 3rd party or offsite facilities are provided by customers with input from Teladoc Health.

MIMPS (previously "PACS") Configuration Requirements

1. Appropriate software version or options enabled on MIMPS
2. Responds to DICOM query/retrieve without altering information (e.g., C-FIND receives expected UID information)
3. Network connectivity with Imaging server is capable of transmitting radiology studies in a timely, reliable fashion (such as 200 images in 10 seconds).