Cisco Approach to Telehealth

A Viewpoint from the Cisco Healthcare Business Transformation Team

Jason Mortensen
Healthcare Managing Architect

July 2015
# Table of Contents

1. **OVERVIEW** ................................................................. 3
   1.1. Telehealth Trends and Statistics .................................................. 3
   1.2. Versions of Telehealth .................................................................. 4
   1.3. Terminology .................................................................................. 4

2. **DEFINING YOUR OPERATING AND FINANCIAL STRATEGY** ................. 5
   2.1. Define Your Business Scenarios and Use Cases .................................. 5
   2.2. Understand and Build the Financial Model (Including Reimbursement) ........ 5
   2.3. Identify the Business Outcomes and Value Metrics ............................... 7
   2.4. Physician & Clinician Licensure ...................................................... 8

3. **PLAN YOUR DEPLOYMENTS** ....................................................... 9
   3.1. Organizational Needs ................................................................... 9
   3.2. Defining a Desired Workflow ........................................................... 10
   3.3. Technical Requirements .................................................................. 12
   3.4. Defining a Project Champion ............................................................ 12
   3.5. Training Requirements .................................................................... 13

4. **ARCHITECTURE COMPONENTS** .................................................... 14
   4.1. Cisco’s Approach to Telehealth Architecture ......................................... 14
   4.2. Core Network ............................................................................... 15
   4.3. Cisco Collaboration Foundational Infrastructure .................................. 18
   4.4. Choosing an Endpoint ...................................................................... 24
   4.5. Workflow Software .......................................................................... 26
   4.6. Security ......................................................................................... 27
1. Overview

Telehealth is a key initiative for healthcare organizations today. The Cisco Healthcare Business Transformation team (BTX) consults with customers across multiple services lines including Neurology, Behavior Health, Cardiology, Dermatology, post-procedure follow-up, acute care, and patient outreach just to name a few. BTX also finds several reasons for why organizations are looking to deploy a system including:

- reducing costs,
- improving patient services,
- avoiding hospital readmissions and associated Medicare reimbursement penalties,
- providing improved access to specialists,
- educating patients, and
- expanding the geographic footprint of the organization.

These use cases and deployment reasons are far from a complete list but should serve as an example as to how broad the telehealth conversation can be and shows the vast number of use cases that can be addressed.

When engaging with customers Cisco often finds that they are in a current state of limited deployment in a small handful of areas across the organization but that they typically lack a unifying strategy or architecture to be able to accommodate a telehealth deployment at scale. These limited or siloed deployments were often a result of direct purchases made by the individual department and often the purchases were completely or partially funded by a grant. In these situations, it is often found that the systems lack technical and workflow interoperability with other video systems, are costly to expand, or do not have the flexibly to use multiple different endpoints to deliver that video session to the end user. Very few customers have what could be called a scaled deployment that is effectively deployed, marketed, has a high utilization rate, or could even resell its telehealth services to other organizations.

This is where Cisco can be a trusted advisor with customers by helping them to establish a vision and architecture strategy for deploying a telehealth program at scale. This starts with defining the needs of the organization and then once those needs are defined a unifying architecture approach can be developed that addresses the use cases that are identified today and also is flexible enough to handle the needs of tomorrow. This is all done through building an architecture foundation were one can add on the individual endpoints and software to fulfill a particular use case and do that cost effectively as well as have the security required for a healthcare architecture that is involved in transmitting Patient Health Information (PHI). This unified approach also provides interoperability and helps to reduce the IT support and administrative overhead of managing multiple disparate systems. Lastly, the system is nothing if it does not deliver a value to the business, and thus defining and measuring the value is paramount to a successful deployment.

This white paper is intended to provide an overview of Cisco’s approach to telehealth deployments and provide high-level guidance. It is intended for an audience that has a broad understanding of Cisco’s communications architecture and technology. It will reference additional material that provides far more technical detail and design recommendations, but this document is not intended to replace Cisco’s CRDs or similar documents and the guidance from those documents should still be followed as it concerns the actual deployment, setup, and maintenance of the Cisco architecture components.

1.1. Telehealth Trends and Statistics

It seems that any consulting company report that you read predicts an explosion of electronic visits. The common theme across all studies is that with looming physician shortages, insurance coverage expansion (associated with the US state and federal insurance exchanges) and increasing consumer demand for convenient care, telehealth will grow significantly. Cisco also sees a large driver for telehealth with shifts in reimbursement dynamics moving from volume to value based reimbursement which has created a greater sense of urgency to reduce costs and maximize operational efficiency. Telehealth programs provide a great way to achieve both of those goals simultaneously.

Some examples of data from the industry include:
• Deloitte¹
  o There will be 100 million e-visits globally in 2014, up 400% over 2012.
  o Most of the e-visits occur in North America, with 75 million, or 25% of the addressable market.
  o There are 600 million annual primary care visits in North America with half for problems that could be handled with e-visits.
  o 2014 is an inflection point due to changes in technology and industry pressures to lower cost and improve care.
    ▪ Pervasive PC deployment
    ▪ Ubiquitous Internet access
    ▪ Increasing tech comfort by older adults
    ▪ Mass adoption of mobile devices

• SG2²
  o By 2024 15% of all US evaluation and management visits will occur virtually.
  o 70% of surveyed patients reported being comfortable replacing select in-person visits with texts, email or video.
  o By 2023 17% of Evaluation & Management visits will occur virtually.
  o By 2023 262 million visits will be conducted virtually.

1.2. Versions of Telehealth
While the term telehealth is used in this paper there are several emerging terms for the same concept such as:

• e-health, e-visits
• connected health,
• telehealth, or
• virtual health.

Additionally, when you look at the technology involved or versions of telehealth, you have voice, chat, video, email, mobile applications, and geo-tagged devices. The visits can also be asynchronous -- patient data and information is captured and exchanged between the patient and provider but it is not done as part of a real time consultation; or synchronous –is essentially a real-time exchange of information.

This paper is strictly focused on synchronous telehealth sessions primarily involving video but also possibly including voice or chat. While other technologies and systems may be part of an architecture strategy and thus need to be included in the planning, those other technologies and systems are too numerous to be able to cover in this white paper.

1.3. Terminology
The following terms are used this paper:
• Care Provider – Any employee or affiliate of the healthcare organization that will be involved in delivering the services in the telehealth session. This could be any role but common ones are a physician specialist, general practice physician, physician assistant/nurse practitioner, behavior health specialist, or a translator.
• Clinical Leader – Person in a leadership role of a particular service line. Typically a manager, director, or senior physician. This person will typically also be in a decision-making capacity about the technology or how it is used.
• Scheduling Agent – Person that is responsible for manually determining availability and scheduling the providers and/or patients required for a telehealth consultation.
• Patient – Any individual receiving care from a Care Provider.
• Telehealth – A remote engagement and exchange of information between a patient and a provider using some sort of technology.

² “Virtual Health: Aligning Solutions With Enterprise-Wide Priorities” by SG2 Intelligence, 2014
2. **Defining Your Operating and Financial Strategy**

At the start of any telehealth initiative, one must first define what issues you are trying to solve, situations you are looking to address, and outcomes you are looking to achieve. As noted in the overview section, the business situations and desired outcomes for a telehealth deployment are as vast as the topic is broad. This section of the document will go over the model that Cisco follows to guide our customers when consulting with them on a strategy. The first step is to understand the overall strategic imperatives that a telehealth program will address. For example, is the overall corporate strategy to expand access to care, to expand into different markets with new offerings and partners, or to target specific cost savings across the organization?

A **Chronic Care Model** is a strategy that targets specific populations (having a common disease-state, e.g., diabetes) that currently consume the majority of high cost services. Example care models will include mobile and home care, outreach programs, patient-centered medical homes, pharmacy management, centers of excellence, and specialty clinics in hospital settings.

A **Primary Care Support Model** is a strategy that primarily targets expanding access to care. This approach leverages the significant investment in resources and expertise of the entire health system, especially if that health system owns many assets as part of an overall continuum of care. Some examples include retail clinic support, urgent care clinic support, diagnostic imaging centers, complementary medicine, specialty hospitals or units, and centers of excellence.

A **Wellness or Prevention Model** is a strategy that starts with the revenue and cost models at the forefront. This would be appropriate for a Payer, ACO, or Health System managing populations in a value-based reimbursement scenario. The goal may be to demonstrate cost savings for a patient population, while also closely managing the revenue and cost for the provider organization. For example, a provider organization may wish to establish outreach programs in partnership with a Payer, partner with large self-funded employers to offer remote care for employees from a campus based health center, or target industries with remote locations where travel is difficult and costly.

The model selected likely results from the goals and objectives of the organization. Is the overriding objective to manage costs and increase efficiency, or is it to build a new revenue stream? Determining the strategic objectives and the supporting model or models will go a long way towards helping the organization define the appropriate success metrics later.

2.1. **Define your Business Scenarios and Use Cases**

Once the overall strategy and objectives are defined, the functional areas within the organization will refine the specific scenarios. For example: Acute Care eVisits, Stroke (emergency, or pre & post procedure), Dermatology, Behavioral Health, Pharmacy, Specialist Consults, Patient Education, Staff Education, Grand Rounds, or Language & Interpretative Services.

There are many detailed use cases that fall within each of these scenarios that will require analysis and planning for new business processes and workflows for clinicians as well as patients.

2.2. **Understand and Build the Financial Model (including Reimbursement)**

In most cases finances are the key consideration of the organizations’ imperatives and telehealth programs and therefore it is important to be able to measure results. In the exercise of defining business scenarios and use cases, the organization will identify specific desired business outcomes. Most of those business outcomes will have some sort of financial consideration tied to them.

The old adage holds true – “You don’t always get what you want – but you most often get what you measure!”

To ensure this is achieved, you need to identify the measurements that contribute to the business objectives and imperatives associated with the program. If you are targeting one of the operating and financial strategic models described above, show how you will measure desired strategic contributions (e.g., physician productivity, reduced costs, increased access, increased revenue, attraction of new patients, etc.). Other examples include increased patient satisfaction, customer retention and loyalty, or overall population management success.
If you are targeting a cost savings model, show the key metrics and benchmarks that you are improving. For example, this could be reduced travel costs, reduced training costs, or reduced staff overtime. If this is a revenue growth initiative, define the ways telehealth can drive additional revenue or new patients into the organization.

2.2.1 Insurance Reimbursement for Telehealth Services

Telehealth reimbursement is a very complex topic, varies by state, and going into detail on the topic is beyond the scope of this whitepaper. At a high level in the fee-for-service (FFS) model there are three payer categories: Medicare, Medicaid, and Commercial Insurance from private payers. Examples of Private Payers include Blue Cross Blue Shield Plans, Aetna, Cigna, Humana, and United Healthcare to name a few. These organizations serve both individual policy-holders and employer groups. When employer groups are large, they often self-fund their benefit plans to their employees, and they use Private Payers to help them administer these benefit plans.

Reimbursement rules for Medicare involve, among other things, the site where the service is originated from, the type of service offered, and rural health professional shortage areas (HPSAs). A good rural health fact sheet from CMS can be found at http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/telehealthsrvcsfctsht.pdf. Also CTeL has a very good reference page at http://ctel.org/expertise/reimbursement/. These are among many sites and resources available to get more information on telehealth reimbursement policies.

Reimbursement for Medicaid varies state by state. Again the CTeL site is a fantastic resource for state specific laws http://ctel.org/expertise/reimbursement/. A breakdown of state telemedicine legislation tracking can also be found from ATA at http://www.americantelemed.org/docs/default-source/policy/state-telemedicine-policy-matrix.pdf?sfvrsn=62.

Lastly, in the reimbursement realm there are Private Payers. In this area not only will there be variance from payer to payer, but also from individual hospital contract to contract. Private Payers set their own reimbursement policies as it relates to telehealth services, however, they carefully track and observe what federal and state programs do and typically follow suit.

It should be noted that in healthcare there is a gradual shift from “volume-based payment” (fee-for-service models) to “value-based payment,” which may include pay-for-performance, bundled payments, or capitation. In these models, reimbursement for an individual telehealth session is not as much of a factor as having a telehealth program that helps manage the care of the patient via a high-quality and cost-effective solution.

One last form of reimbursement includes out-of-pocket direct, or cash, payment by the patient. With the increase of high deductible insurance plans the industry is seeing an increased number of instances where patients are paying much closer attention to the cost of care they are about to receive and balancing that with quality, ease of scheduling, and convenience of the visit. This new choice paradigm for consumers is often called the ‘retailization of healthcare.’

2.2.2 Productivity

Monetary reimbursement should not be the only consideration when looking to deploy a telehealth program. There can also be a strong case for productivity enhancement for employed physicians, and thus with increased productivity can come increased revenue from greater patient throughput and/or increased job satisfaction on behalf of the employed physician. This productivity increase most often comes from the reduction in travel time to see a patient or a more efficient schedule due to shorter duration telehealth visits. If a physician is traveling one hour, one way to a remote clinic in order to see a select few patients that ends up being two hours of unbilled and nonproductive travel time that could be eliminated with a telehealth deployment.

2.2.3 Telemedicine Parity Laws

One area where Cisco sees positive legislation trending is the passage of telemedicine parity laws in states. Specific language will vary state-by-state, but in general these laws require that private insurers reimburse the provider for a telemedicine visit at the same rate that they would for an in-person visit. Seventeen states have passed and adopted telemedicine parity laws in their respective state legislatures over the past few years. An additional 14 states have proposed telemedicine parity legislation up for review/vote this year. Below is a summary graph from ATA that can be found at http://www.americantelemed.org/policy/state-telemedicine-policy#.VFOn9IvF_Nc.
### 2.3. Identify the Business Outcomes and Value Metrics

Once the financial model and reimbursement details have been understood, the next step is to identify the desired business outcomes and their associated value metrics. This process starts by defining the relationship map between the business scenario, the detailed use case being addressed, the desired business outcome, and finally the metric used to identify the value associated with the flow.

In the example below, an organization is planning to implement a Telesstroke program that links a stroke specialist at their main (“hub”) hospital and the emergency team at their remote (“spoke”) hospital. They are looking to achieve two specific business outcomes: increased admissions of stroke patients at the remote hospital and increased follow-up rehabilitation of those patients using specialists at the “hub” hospital. The financial or value measurements are tied to increased revenue and utilization of staff for the stroke treatment program at the remote “spoke” hospital.
2.4. Physician & Clinician Licensure

Like reimbursement, the full scope of state medical licensure is a complex topic that is outside the scope of this document. It is brought up here as it is a common issue and question raised. As the laws stand right now, a provider must be licensed in the state where the patient is located and treated. This ends up being a major barrier for delivering telehealth services across state lines but may be resolved at a later date via currently pending federal legislation.
3. Plan your Deployments

At the start of any design one must first define the issues you are trying to solve for, use cases you are looking to address, and outcomes you are looking to achieve. Once the use cases and desired outcomes for a telehealth deployment have been defined, the task of prioritizing the deployments is the next logical step. This section of the document will go over the approach that Cisco follows to guide our customers when working with them on an implementation and deployment. While not a complete list, the most common areas, questions, and information to be gathered includes:

- Define the functional needs within each organization affected;
- Define the desired changes needed within the workflows and processes;
- Define and understand the technical requirements;
- Identify and define roles for Project Champions; and
- Identify and define training requirements.

The most common service lines that Cisco sees our customers looking to address are (in no order of importance):

- Telestroke consultation,
- Other Neurology consults,
- Primary Care eVisit (sore throat, flu, headaches, etc.),
- Cardiology pre- and post-procedure consultation,
- Dermatology,
- Behavioral Health,
- Patient Education / Video Coaching,
- TelePharmacy,
- Specialist Access/Consultations to Remote/Rural Facilities,
- Grand Rounds Simulcast,
- Interpretative Services,
- Patient Triage done through a Contact Center.

3.1. Organizational Needs

The first step to any deployment is defining what the project is intended to achieve. While this may seem like an obvious statement, Cisco often finds that there are mistakes or items overlooked in this critical first step.

One common approach that limits program options for the organization and prevents the scalability and interoperability of a telehealth program is when a deployed solution is designed for a single use case, instead of designing a solution for the organization that will accommodate multiple use cases at scale. In a common scenario, a clinical leader might approach IT discussing a use case they want to address. This is often accompanied by a technical solution that they recently saw at a trade show or read about in an industry publication. In a rush to accommodate the clinical leader, the solution is purchased and deployed without a vision into how it fits into an overall telehealth or remote medicine strategy. In hindsight, this often results in redesign at a later date, as the system is not interoperable with other technologies, is costlier to maintain, does not scale to other uses cases, and/or does not provide an integrated workflow across the care continuum.

Cisco believes this is a prime area for IT-focused resources to be able to show value and be involved in driving a strategic vision and interoperable, scalable solution for the organization. The recommended step here is to contact other clinical leadership, hospital executive leadership, and other stakeholders in the organization to gather their requirements, desires, and initiatives. The exact individuals to engage here will vary from organization to organization with no right or wrong person(s), but the take-away will be to gather a current comprehensive list of organizational goals that can inform the system design.

Gather telehealth requirements across the organization rather than a single department, clinical leader, or service line.
When requirements are gathered it is not only the use case that the original department or leader is looking to address or the overall goals they want to achieve, but also the details around the desired workflow, provider requirements, and other user requirements. Guidance for these other requirements is detailed in the sections to follow.

3.2. Defining a Desired Workflow

A successful deployment of any solution involves unison of People, Process, and Technology. Defining the desired workflow of a telehealth deployment is the Process part of that trio. As is a recurring theme in this white paper, there is no true right or wrong workflow process. In the deployments that Cisco has been involved in, we have seen that every organization has a slight tweak on a process because it works for their users. Those processes can range from a completely software driven model where an automated system is conducting tasks like provider availability, call routing, billing, EMR integration, and so on to a system where pagers are still used to contact the specialist and the same core workflow process is followed with the face-to-face visit replaced with a video visit. The only real mistake is to have a process that is vastly different than existing non-telehealth workflows resulting in a cumbersome, time consuming system that is not used by its stakeholders.

When determining the workflow, understand the existing non-telehealth workflows and try to replicate these as much as possible while still improving ease of use and automation.

Regardless of whether the workflow will be completely automated, completely manual, or somewhere in-between there are several key components to understand. It is not important at this stage to define the exact technology systems that will conduct the tasks; however, it is important to define the desired functionality. In fact, some may argue that it is even detrimental to brainstorming at this stage to confine ideas to just what a current deployed system is capable of.

- **Scheduling** – At a high level scheduling has two sides.
  - The first is the side of the care provider and at the core involves how the telehealth consultation will be worked into their other daily tasks and appointments. The first component is a system that can determine the availability of the provider, and the technology can range from a simple on-call coverage calendar to an automated scheduling system that is integrated with the provider’s calendar in the EMR. The second component is how the provider will see that they have a telehealth consultation scheduled. For a workflow where he consultation occurs relatively immediately and the provider is paged with a request or is monitoring an active request queue, this is not applicable. However in most deployments the consultations are scheduled for a future date. In practice with these scheduled events Cisco has found that the best approach is to have a single schedule as the source of truth, preferably the calendar in the EMR, but there are other possibilities such as using a Microsoft Exchange supplemental calendar. Also, it should be discussed who will do the scheduling. Cisco most often finds that it ends up being the same people or department that conducts scheduling for in-person visits, but depending on the use case there may be other completely integrated and automated systems integrated with the Cisco Contact Center that can determine skill based routing and availability.
  - The other side of scheduling is the patient facing side. In some use cases, the patient may not be the one actively making the scheduling request but instead someone on behalf of the patient initiates the request. One example of this is a nurse requesting a behavior health consultation for a patient in the ER. Again depending on the clinical area and use case there are many options here from viewing an existing electronic calendar, an integrated system to determine whom the specialist on-call is and routing the request to that specialist, or even having the patient be able to schedule an appointment themselves directly through a web patient portal or mobile application.

- **Reason for Visit** – How will the symptoms or reason for the visit be inputted and communicated to the care provider? From a workflow side, this can provide the benefit to the provider of knowing why the request is being made, so they can be prepared to handle the consultation. From a technology integration standpoint, as will be discussed in this paper, the reason for visit can be a factor in being able to automatically route and queue the request to the provider who can best handle the case.

- **Notification of Appointment Request** – In use cases where someone on the patient side will make a request for an appointment to be held sometime in the future, how will a scheduling agent be aware that a request was made, so they can formally schedule the session? If there is an automated means of scheduling, how will the provider know that an appointment has been scheduled? Lastly does there need to be a final confirmation sent to the patient?
• **Queuing** – In certain use cases there can either be more than one request made at a time, or even when there is a single concurrent request, there may be a need to have the patient placed in a “holding queue” while they wait for the care provider to join the session.

• **Medical Device Integration** – Will the use cases require the use of medical devices such as an otoscope or stethoscope? There are a limited number of telehealth use cases that require medical devices, but if they are required, there will be an important impact on the technical design. If medical devices are required other questions need to be addressed including:
  o Does the output of the medical device need to be transmitted across the video session?
  o Will the readings of the device need to be automatically or manually inserted in the EMR?
  o Are outputs, such as pictures, required to be permanently stored and part of the patient’s record?

• **EMR Integration** – The need to able to accomplish EMR related tasks, like viewing the patient’s history and entering findings, is likely given in most use cases of a telehealth deployment. When planning for the telehealth design requirements, it is key to know the functions that have to be completed in the software interface that is part of the telehealth deployment thus supporting a single user interface point for the providers during the session. These functions will then need to have information transmitted to and from the EMR, likely though an HL7 or API interface. Depending on the use case, integration into the EMR may be ideal, but for many use cases Cisco finds that organizations are taking an approach to workflow that video is the next in-person meaning that you have the same workflow in telehealth as you do for an in-person visit. In this scenario the provider has the EMR on a separate screen or PC where they are then entering the data directly into the EMR as they would during an in person visit.

• **Billing** – Does the use case require the need to bill the patient directly through a portal? The most common area where Cisco sees this requirement is the eVisit Acute Care use cases where the patient is paying a deductible or a per-visit flat fee. When one looks at the requirements for billing, how the payment will be processed is really the last step in the workflow requirements. If you want to implement payment before service, then you need to understand items including:
  o Is this patient and the type of request/need even eligible for an eVisit consultation?
  o What is the patient’s health insurance plan and does it cover the cost of the visit?
  o Is this visit in part of a bundled payment for a procedure and thus payment has already been includes as part of a larger bill?

If the desire is to have payment issued after services are delivered, similar to an inpatient model, then billing may be handled by the same processes and workflows, as those used for in-person visits.

Note that this section just covers the topic of billing the patient. Reimbursement through various insurance plans is outside the scope of this document, but some additional detail is noted in the [Understand and Build the Financial Model](#) section of this document.

• **Pharmacy, lab, or other system integrations** – Do you need the ability to place lab orders, order prescriptions, or other CPOE tasks as part of their use cases? If so, will this be done directly though the EMR system, or will it require all orders be placed through the telehealth software and integrated with the EMR?

• **Specific Specialty Needs** – Are there specific workflows or functionality that is very specialized and required for that use case? A common example of this is in Telestroke where one may want a system that includes an assessment questionnaire to help determine if TPA should be administered.

• **Home Monitoring Device Integration** – In the use cases where a care provider will be doing consultations to the patient in their home, will there be a need for home monitoring devices such as blood pressure, blood sugar, pulse oximeter, or scale? If these devices are required, you will need to determine where the data from these devices will be sent and stored and what integration, if any, is required with the EMR or telehealth software. There are many vendors in the home device space, and most often these devices upload and store the data to their private cloud where it is then available for the provider to reference during the consultation; however, this data is not directly sent to the EMR and rarely integrated into the telehealth software interface.

• **Individual’s Location** – Where will the provider and patient be located? What are the mobility requirements for these respective individuals? Gathering this location information in the workflow will then be used as a major factor influencing the required equipment and overall back-end architecture components.

Gather the requirements for how the targeted users will use the system and what functionality they will require to achieve their needs.
3.3. Technical Requirements

In addition to workflow requirements that were highlighted above there are some additional possible requirements that are more technical in nature.

- **Voice, Chat, and Video** – Often when one thinks about telehealth they think in pure video terms. However, customers may think of telehealth in terms of chat or voice instead of, or in addition to, video. Voice or chat may also be a supplement to video and can be used before a video session is started or in the event that there is a problem with establishing a video session or the quality of the video session.

- **Skill based routing** – When a person makes a request for a telehealth session, how will that request be routed to the best-qualified and currently available person? This may start with a Reason of Visit request as noted in the workflow section where a person enters why they want the consultation. Based on that request, a manual or automated system is used to route the request. There may also be no additional skill-set routing required like in the case of a Telestroke where only the on-call neurologist is needed. However, even in this case availability routing is still needed to determine who that on-call person is and if they are available to take a consultation.

- **Notification of waiting patient** – In the event that queuing is used, how will the provider be notified that a patient is waiting for service? Commonly, Cisco will see a page send or perhaps an automated phone call placed.

- **Patient registration** – If the system will be used to conduct telehealth visits for patients that may not currently be members of the health system, how will new patients be registered? If it is an existing patient, do they need a user name/password to be able to access the portal or application that a visit will be conducted from?

- **Document sharing** – Are there any needs for document sharing or co-browsing during the session?

- **Recording** – Is there a need to record the session? If recording will be used, is there a need for the patient to be able to access that recording at a later date? Where will these recordings be stored? What authentication mechanism will be used to control access to the recordings?

- **Endpoints** – Far more detail will be provided in Architecture Components section of this document but in general here one should think about the requirements for delivering video to the respective parties. Questions here include:
  - Will video sessions be made to parties outside the organization’s secure network?
  - Is web browser integrated video required?
  - Is video required to be integrated into a mobile application on a table or smart phone?
  - What devices will the provider use and what are the mobility requirements for the provider?

Gather the more non-workflow related technical requirements.

3.4. Defining a Project Champion

In the telehealth deployments Cisco has witnessed that it is hard to find an example where the deployment was a success without strong project champions involved. This paper defines three champions: a Clinical Champion, IT Champion, and Telehealth Champion.

3.4.1 Clinical Champion

In our view, the most important person is a Clinical Champion. This person is often a provider that is part of the service line where the system will be implemented, but that is not necessarily a requirement. This person should have a very strong understanding of the workflow and challenges that are part of that service line and must someone that is respected by the individuals in that area. In the planning stages, this person will help define the workflow and technical requirements, review the new proposed workflow, may review the architecture components but especially the endpoints, help to determine project success metrics, and help determine the training plan that will be used. During implementation and rollout, this person will also assist with the training, monitoring of success, and various workflow and technical tweaks that will likely need to be made.

One can argue that the most important role of this position is to be a champion of change. As noted in the introduction, every system deployment involves people, process, and technology, and the clinical champion can help with all of those but is especially influential with people. Humans are naturally resistant to change and the champion can assist with addressing
user concerns, describing the value of the program to the organization and individual, and serve as the go-between for the users and the larger project team.

3.4.2 IT Champion
The second role is the IT Champion. This person will be responsible for leading the technical components of the solution assessment and implementation. Cisco finds that the best person for this position is the Manager or Director who is responsible for the organization’s video and communications infrastructure. As with the other roles, this person needs to be a change agent. This person should be a partner with the clinical teams and be focused on ways IT can deliver business value to their users.

3.4.3 Telehealth Champion
The last role this paper defines is a Telehealth Champion. Many times this is not a separate role but part of the responsibilities of the Clinical or IT Champion. However some larger organizations have hired a person who is solely responsible for the adoption and deployment of telehealth. Along with a change agent like the other roles, the role of this person will be to make sure a particular deployment is in line with the organization’s overall strategy. Depending on the person in this role they may also be responsible for defining the strategy, determining best practices for roll-outs, and assisting with internal communication to applicable stakeholders.

To help with a successful deployment, make sure the organization has defined project champions.

3.5. Training Requirements
During the planning of the deployment of the solution you should develop a plan for training. This includes:

- Who needs to be trained in both clinical departments and IT supporting departments?
- What supporting documents are needed to supplement in-person training?
- Are their super users identified that will serve as train-the-trainer targets?
- Who will deliver the training?

In training keep in mind that there are two components: training on the technology and training on the workflow.
4. Architecture Components

Once you are at the point where you know what use cases you want to address today and in the known future, the proposed workflow for those use cases, and the desired features that will be required, it is time to put together the architecture components to address that solution. Overall, Cisco’s architecture strength is the use of a foundational open standards communications infrastructure that can not only serve multiple use cases for telehealth but also provide video, voice, and chat services for the organization’s other internal and external communications use cases. The Cisco collaboration architecture also provides a highly available infrastructure with integrated security that can be deployed on premise, in the cloud as a hosted environment, or in a hybrid deployment.

4.1. Cisco’s Approach to Telehealth Architecture

The diagram below explains Cisco’s high-level approach to an architecture strategy for Telehealth.

As you see in this diagram, like a good foundation of any physical structure you start from the ground up, building layers on top of each other with each layer providing services to the one above it.

Network & Compute Infrastructure – The foundation of any IT system contains the route/switch and wireless infrastructure that will quickly transmit the data securely from one location to another and any compute components (servers) that will house the applications that provide the service’s functionality. The ‘Core Network’ section of this document describes recommendations for this level.

Collaboration Services – Video and communications back-end servers build on the Network & Compute Infrastructure. The exact components/servers required here will vary depending on the use case, but at a high level, the functionally provided includes endpoint registration, video session establishment and communication both inside the network and outside a firewall, scheduling, bridge management for sessions with more than two endpoints, managing the viewing experience across multiple endpoints with varying number of screens or resolutions, and recording as well as distribution of the video sessions. Additional detail on this level is found in the ‘Cisco Collaboration Foundational Infrastructure’ section of this document.

Applications & Devices – At this level you involve the end user facing components. Here you can leverage the depth and breadth of the Cisco endpoint portfolio, where there are endpoints ranging from video integrated into a web browser or
mobile application, Jabber as a software client across a suite of operating systems, video phones, personal desktop and portable units, and room based systems. In addition, Cisco’s partners manufacture mobile carts to address specific use cases.

There are a few very important Cisco strengths here as it relates to the specific endpoint. The first is the flexibility to pick the endpoint that is the best for that particular use case. When you expand to other use cases you can simply use the same or different endpoint for that new use case depending on the specific needs. The second is having full interoperability and feature parity across the entire line. Thus a mobile application integrated video client on the “low” end can communicate with a fully immersive room based system on the “high” end and all the endpoints in-between. The third point is that these systems and endpoints are not just for telehealth but can accommodate multiple uses. For example, one can use a DX80 in the morning to conduct a telehealth session, use it later in the morning to call into a video bridge for tumor board, and then use it later in the day to have a video chat with a colleague to consult on a case. That same DX80 can also be used as a desktop monitor for a PC/laptop thus reducing the number of devices and clutter on a deck.

From a design and use case standpoint, more often than not, you can stop at this point. Most use telehealth cases simply involve connecting one person to another replacing an in-person visit with a visit over video. Even in the cases where medical device integration is required, many times that is just displaying the output from the device, like an exam camera, over the video channel and integration to other workflow software is not required or would only be implemented at a later phase. For these situations where the features of a workflow software are not needed, the design can stop at this device level. Additional guidance on selecting endpoints is noted in the ‘Choosing an Endpoint’ section of this document.

**User Experience** – There are also use cases where additional workflow software is needed. Additional functionality like integrating billing, virtual queuing, EMR integration, e-prescriptions, and skill based routing is required. In this case, you then add on additional workflow software from Cisco or one of our partners. It is important to continue with the foundational architecture and building blocks in that the workflow software leverages and integrates with the same endpoints, services, and infrastructure that they have already purchased and deployed. Again, Cisco’s approach gets away from a siloed deployment where one has a telehealth and communications system design that only serves one or a small handful of use cases, is difficult to manage, and does not scale. Additional guidance on workflow software is noted in the ‘Workflow Software’ section of this document.

**Fundamentals** – Along the right side of this diagram, notice that there is security and unified management incorporated into all levels of the stack. While this paper will not do a deep dive into Cisco’s security infrastructure, it will discuss some considerations in the ‘Security’ section.

**Deployment** – Lastly, across the stack there are multiple deployment options. You can deploy all the infrastructure on-premise, in the cloud, or a hybrid of the two depending on the needs and policies of the organization.

### 4.2. Core Network

As noted previously, this layer contains the route/switch and wireless infrastructure that will quickly transmit the data from one location to another and any compute components (servers) that will house the applications that are providing the services functionality. This section of the document will not focus on the compute components, although Cisco UCS can serve as an amazing x86 compute platform, but rather recommendations to take into account with the highly available route/switch and wireless infrastructure with security built in.

#### 4.2.1 General Bandwidth Requirements

Customers frequently ask Cisco how much bandwidth these video sessions will consume on the network.

**Cisco Core TelePresence** – As it relates to TelePresence, video bandwidth can vary significantly depending on which video codec standard is used. This paper will not go into detail on the standards but rather the data provided assumes that H.264 is used. It should be noted though that H.265 functionality is being built into the newer Cisco endpoints including the MX and DX series and if H.265 is used, the bandwidth required will be reduced by approximately half. However, at the time this paper was written there needs to be feature additions to our infrastructure components to support H.265.

Cisco’s IT department offers this advice and speaks to the planning Cisco does internally for the large amount of video traffic on our network.
The bandwidth required differs depending on which video devices are used. The amount of bandwidth needed by video increases when you move from WebEx Meeting Center video (lower definition), to Jabber and IP video phones (99xx), all the way up to personal TelePresence and immersive TelePresence.

There are some guideline bandwidth numbers listed below, but note that in these numbers it is the utilization of the bandwidth when the session is active. For example, when it is said that a 1 screen TP unit at 1080p used 4.5 Mbps that is when the video session is active and should not be read as a number that is a constant drain on the network. This is a factor in planning as say you have 4 1-screen units. If only one is ever used concurrently the overall bandwidth requirement would be 4.5 Mbps but if all four will be used concurrently the requirement bumps up to 18 Mbps if they are all on the same network segment or primary circuit. Also note that these are recommended values giving the highest possible resolution and frames-per-second (fps) that the device is capable of. The endpoints can operate at a lower resolution and fps and that would then decrease the bandwidth used. However, Cisco believes for telehealth that the highest resolution and fps should be used to provide the best possible experience.

- 3-screen TP room at 1080p – 16.7 Mbps
- 1-screen TP at 1080p – 4.5 Mbps
- 1-screen TP at 720p – 1.68 Mbps  Note: The new MX endpoints require less bandwidth with H.265
- EX-90 at 720p – 1.5 Mbps  Note: The new DX endpoints require less bandwidth with H.265
- Jabber Client or Jabber Guest – 720 kbps
- Remote Expert Mobile – 1-2 Mbps depending on the endpoint

WebEx – When using video in a WebEx session, our WebEx team generally recommends network bandwidth above 1Mbps per participant. The minimum network bandwidth to view video should be above 320Kbps per participant.

- High Quality - 360p (640x360) - Up to 1.5 Mbps
- Standard Quality - 180p (320x180) - Up to .5 Mbps

Note: The figures above are only for webcam video and do not include any other in-meeting activities. You will need to additional bandwidth to use desktop sharing, integrated VoIP, etc.

4.2.2 Quality of Service (QoS)

Video is unique in the network, because most of it exhibits one or more of the following characteristics:

- Inelastic - no packet loss acceptable, no ability in the application to throttle the sender due to congestion based traffic loss
- Live / real-time - low latency and/or jitter requirements
- Highly compressed - often requiring low packet loss

QoS can mean different things to different audiences. To an end user it means there are no dropped calls, no static, and the video is high quality and smooth. To a network manager they are focused on metrics like controlling delay and jitter, reducing packet loss, and controlling the used vs. available bandwidth.

We recommended configuring QoS to ensure that it will support all voice and video, while regular data services like email and web browsing will be significantly impacted. It is felt that voice and video are critical services, especially for telehealth, while data services can tolerate the rare delay.

There are multiple design recommendations for QoS and each network and situation will be slightly different. Some reference materials that may be helpful are:


Cisco Services can be engaged to analyze and recommend specific configurations for your network regarding QoS.
4.2.3 Wireless Network

Video over wireless
Extending video over a wireless network has certain challenges compared to a wired network. These challenges arise because a wireless network introduces a set of performance characteristics that oppose some of the traditional approaches to Quality of Service (QoS). These challenges can be characterized as Variable Data Rate, Packet Loss, & Multicast Unreliability.

Variable Data Rate
One of the differences between a wireless and a wired LAN is that the data rate of transmission over wireless varies over time, depends on the distance of the client from the access point, and depends on the number of active devices communicating with that AP at any given time. This is not the case with a traditional wired LAN in that if a wired connection is operating at 100 Mbps today, it will operate at 100 Mbps tomorrow. As a result of these variations in data rates, the throughput of individual video flows and the capacity of the overall network changes with time. In some sense, sending video over a wireless network can be similar to sending video over the public Internet where throughput and the user’s experience can vary wildly over time.

This variable throughput and capacity present a challenge to the traditional QoS approach of bandwidth reservation and admission control. The most common method for identifying video streams is through the use of differentiated services code point (DSCP) markings in the IP header. The drawback of using only DSCP is that it does not provide an easy opportunity for the infrastructure to employ admission control since there is no explicit request for admission.

Another method for implicitly indicating a video stream is for the infrastructure to support a configuration of certain IP address and port combinations that are known to be used for video. For example, an enterprise might have an internal video server used for corporate communications or training. Traffic from this server could be marked as video.

Packet Loss
Another difference between a wireless and a wired LAN is the relative unreliability of the underlying layer 2. Simply put, a wireless network loses a lot more packets than a wired network. When two wireless devices attempt to transmit at the same time packet loss results from collisions. A wireless LAN uses a shared half-duplex medium, and while the “listen-before-talk” medium access method tries to avoid collisions, they cannot be totally prevented. In addition, non-WiFi devices may operate in the same band, most of these devices do not adhere to the “listen-before-talk” algorithm, and so collisions are common.

Another reason for packet loss is that wireless transmissions are subject to fades (short-term signal loss). These fades can be due to absorption or reflections from intervening objects in the environment accidentally causing signal cancellation. A third and smaller factor in packet loss is that WiFi systems hunt for the best transmission data rate by trying different rates and some packets are lost during this search process.

Given the combination of collisions, fades, and data rate selection, it is not at all uncommon for wireless networks to operate with an underlying packet error rate that can approach 5 percent. To compensate, WiFi uses a retransmission mechanism whereby packets that are not successfully received and acknowledged are resent. Even after retransmissions, the final packet loss rate is still much higher than what is typically observed on wired connections.

To provide reliable video over WiFi, a better more reliable physical layer can result in higher data rate and fewer retransmissions so that video streams operate more smoothly. 802.11n provides some important advantages in the quality of the WiFi physical layer. Through use of multiple-input multiple-output (MIMO) antenna technology, 802.11n essentially provides a higher level of signal-to-noise ratio (SNR) than previous versions of 802.11. This improvement in SNR can then be applied both to allowing for higher data rates (more throughput) and increasing the reliability of the link (less retransmissions due to fading and rate selection).

The WiFi protocol has a number of features that can improve video performance. The MAC layer contains WiFi Multimedia (WMM) extensions. These extensions provide for four levels of priority queuing: voice, video, best effort (BE), and background. By taking advantage of WMM, video applications are able to run video traffic with priority over other BE traffic.
802.11ac

802.11ac is an evolutionary improvement to 802.11n. One of the goals of 802.11ac is to deliver higher levels of performance that are commensurate with Gigabit Ethernet networking:

- A seemingly instantaneous data transfer experience.
- A pipe fat enough that delivering a high quality of experience (QoE) is straightforward.

In the enterprise, 802.11ac helps solve some key challenges:

- Delivering network with enterprise-class speeds and latencies.
- High-density environments with scores of clients per AP.
- The increased adoption of video streaming.

The one thing that 802.11ac has in its favor is the evolutionary improvement to silicon technology over the past half-dozen years: channel bandwidths can be wider, constellations can be denser, and APs can integrate more functionality.

Apple Device Roaming

The use of consumer devices such as the iPhone in an enterprise environment with business use cases has created some challenges especially as it relates to video and voice services over WiFi. The largest issue to be aware of happens during an active video or voice session if the device is moving and thus roaming from AP to AP. For multiple technical reasons, the iOS devices can have a multiple second gap when transitioning from one AP to another, and if there is an active voice or video call that can result in the call being dropped. To help address this refer to some best practices detailed in Cisco’s Enterprise Best Practices for Apple Mobile Devices on Cisco Wireless LANs - http://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/bestpractices/EntBP-AppMobDevs-on-Wlans.pdf.

4.3. Cisco Collaboration Foundational Infrastructure

At the heart of the architecture design is the Cisco collaboration foundational infrastructure that is responsible for the server-side tasks.

4.3.1 Core Video Infrastructure Architecture

The main functions of a call control infrastructure are endpoint registration, call routing, monitoring, and maintaining connections. Call control platforms also form the base for network dial plans and options for call admission control. Cisco offers two main call control platforms for interactive video: Cisco Unified Communications Manager (Unified CM or CUCM) and Cisco TelePresence Video Communication Server (VCS). As it stands currently with the Cisco video infrastructure, Cisco is adding more functionality to the CUCM server and moving away from VCS. UC Manager is Cisco’s strategic call control platform for all UC, TelePresence endpoints, and bridge resources moving forward with Expressway providing firewall traversal and interoperability gateway functionality.

Your current video and call control infrastructure is going to vary slightly based on when the system was implemented combined with what has been done for maintenance and upgrades, designs for prior functionality requirements, the layout of your physical locations, and your on-premise vs. cloud strategy. The next section will layout some previous architecture designs, but below is what would be the current greenfield modern architecture.

An idealistic modern architecture
With this architecture you have:

- A single UC Manager cluster that provides converged call control for all forms of real time collaboration clients: voice, video, instant messaging & presence, multiparty conferencing, audio and video recording applications.
- Cisco Expressway that provides enterprise collaboration edge services to UC Manager providing secure communications between an enterprise network and:
  - Cloud conferencing services such as WebEx OneTouch.
  - Business-2-business (B2B) and business-2-consumer (B2C) calling.
  - Remote access for mobile clients.
  - Expressway also provides interworking services for legacy H.323/SIP video devices (VCS Control required to support legacy H.323 and SIP video endpoint registrations) and for Microsoft Lync SIP signaling and media interworking. This way, H.323 and Microsoft are interworked at the edge and the rest of the Cisco UC solution is 100% SIP-based (UC Manager interworks legacy SCCP, MGCP and H.323 voice trunks and gateways to SIP as well).
- 3rd party endpoints like those from Polycom and Microsoft predominantly still on VCS Control.
- Full native any-to-any interoperability between all endpoints and bridges. Ad-hoc bridges under Conductor on UCM with scheduled bridges still on VCS Control.
- Homogenized dial plans. Both numeric and alphanumeric fully supported across most of the portfolio.
- Feature and User Experience consistency across the portfolio.
- TMS is positioned as the TelePresence scheduling and conference management platform going forward, with Prime Collaboration taking over the role of provisioning and monitoring the UC system and endpoints.
- Conductor provides bridge resource management and load-balancing for audio-only, HD video and immersive TelePresence multiparty conferences on the TelePresence Server, and TelePresence MCU model bridges.

### 4.3.2 Architecture Components

As has been noted, the functionality of the specific infrastructure components is changing rapidly from release to release. Instead of detailing the components in this paper, reference the most up-to-date publicly accessible information.

4.3.3 Architecture Evolution

Below are some previous architecture designs that can serve as a reference and may be more in line with current customer deployments.

Circa 2010 – At The Close Of The TANDBERG Acquisition

With this architecture you had:

- TelePresence and UC endpoints typically deployed on separate UCM clusters.
- Limited interoperability between endpoints (TelePresence Server was the bridge between these formerly non-interoperable worlds).
- Lots of product functional overlap in every category: endpoints, call control, B2B connectivity, bridging, scheduling and management.
- Different dial plans (numerical vs. alpha-numeric centric).
- Different methods of provisioning, management, and monitoring.
- Feature inconsistency across the portfolio.

Circa 2011-2013

With this architecture you had:

- TelePresence and traditional UC (telephony and SD video) all collapsed on a converged UC Manager cluster. Former Tandberg endpoints predominantly still on VCS Control.
• Full native any-to-any interoperability between all endpoints and bridges. Ad-hoc bridges under Conductor on UCM with scheduled bridges still on VCS Control.
• Product functionality overlap diminished. Roles clarified but not all consolidation fully realized yet.
• Homogenized dial plans. Both numeric and alphanumeric now fully supported across most of the portfolio.
• Provisioning, management, monitoring coming together. Prime Collaboration growing in functionality.
• Feature and User Experience consistency across the portfolio getting better and better.
• New compelling solutions like WebEx-enabled TelePresence.

Circa 1st Half CY 2014

With this architecture you had:
• All endpoints and infrastructure collapsed onto a converged UC Manager call control with Expressway (C&E) for Remote & Mobile Access to UCM, B2B, and WebEx/Cloud-enabled TelePresence connectivity.
• Multiparty bridging for audio and video for all types of conferences now trunked through UC Manager (TMS scheduled resources still separate from Conductor ad-hoc and CMR resources).
• Jabber now available on Windows, Mac, iOS, and Android using Expressway for VPN-less access to UC Manager and related UC services (directories, presence, visual voicemail).
• Video as a table-stakes feature. Infused in a growing number of applications like Cloud-enabled TelePresence, Unity messaging, Contact Center with new enabling technologies like Jabber Guest and WebRTC, H.265 and Scalable Video Coding (SVC).

Circa 2nd Half CY 2014
With this architecture you have:

- Multiparty bridging for audio and video for all types of conferences now consolidated under Conductor with TMS for scheduling and meeting management.
- Full provisioning of TC endpoint device-specific parameters in UC Manager 10.5.
- Introduction of SVC/AVC and H.265 support in single-screen endpoints and bridges.
- Introduction of Cloud Fusion capabilities. Intelligent Proximity between Squared client and on-premise endpoints.

4.3.4 Remote Access

In several telehealth use cases Cisco sees the need for access from an endpoint that is not physically located within the secure hospital network. These use cases include a patient connecting from their home or a provider conducting patient outreach and running the Jabber client on their tablet or laptop.

Cisco Unified Communications mobile and remote access is a core part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging and presence services provided by Cisco Unified Communications Manager (Unified CM) when the endpoint is not within the enterprise network. The VCS provides secure firewall traversal and line-side support for Unified CM registrations. The overall solution provides:

- Off-premises access: a consistent experience outside the network for Jabber and EX/MX/SX Series clients.

VCS Expressway

Prior to Cisco Call Manager x9.1 the VCS Expressway server was used for firewall transversal for off-premises access. A design would look something like the below.

**Expressway Edge**

With Unified CM x9.1 a new alternative or supplemental option was introduced for video internetworking and firewall transversal and that was Expressway Edge or Expressway-E. As it relates to the topic of this paper, Expressway-E added features to allow remote access without the need for a VPN connection, using AnyConnect for the Jabber client, for:

- Cisco Jabber for Windows 9.7 or later,
- Cisco Jabber for iOS (iPhone and iPad) 9.6.1 or later, and
- Cisco Jabber for Android 9.6 or later.

It also includes VPN-less support for:

- Cisco TelePresence endpoints/codecs running TC7.0.1 or later firmware,
- Jabber Guest, and
- B2B collaboration.

A design would look something like the below in a peer Expressway deployment but also note that Expressway-C/E can run in parallel to an existing VCS-C/E deployment.

4.4. Choosing an Endpoint
Cisco has a suite of physical endpoints and soft clients to fit the needs of a large range of telehealth use cases. Cisco also enables users to use their personal devices running applications or web browsers with integrated video functionality. While this paper will not go into detail on all the endpoints, it will cover what Cisco sees as the most commonly deployed ones for telehealth.

4.4.1 Soft Clients
For purposes of this paper, a soft client is an application program that enables video from a computing device such as a smartphone, tablet, or laptop. Cisco has three clients that come into play in telehealth being Jabber, Jabber Guest, and Remote Expert Mobile.

Jabber
Jabber is Cisco’s software client that enables collaboration anywhere and across any device including those running Android, iOS, Windows, and MacOS.

Related to Telehealth, the primary use cases Cisco sees for Jabber are where the provider is not always, or in some use cases never, located next to a physical endpoint.

Pros:
- Flexibility of the endpoint device being a smart phone, tablet, or laptop. With an enterprise login across those platforms you have a unified contact list, presence, video, chat, and voice messaging functionality all with a consistent look and feel across device platforms.

Cons:
- The Jabber client is intended for employees of the organization. Is not well suited for patients, external physicians, etc. that do not have an account on CUCM.
- The client needs to be downloaded and installed which means it is not the best suited for a one-off video engagement where the employee will not have a regular or semi-regular use of video.

Common Use Cases:
- Provider who is traveling to patients homes, homeless shelters, or otherwise conducting remote patient outreach and travels with a tablet or laptop that they wish to do video consultations from.
  - Cisco often gets questions about connectivity when the provider is mobile and outside of the hospital’s premises. Most often in this case a cellular mobile access points (Mi-Fi) is used and with adequate bandwidth with a 4G/LTE signal generally video quality issues are not seen.
- Providers who are traveling around the hospital and are not commonly located at a desk or other location that has a physical endpoint. Note due to wireless roaming issues when using iOS devices, it is not recommended that the video session be held while the provider is still moving and thus roaming from AP to AP.
- Providers who are employees of the hospital and want to have a video session from their tablet or laptop but don’t conduct enough sessions or need the functionality to legitimize a physical endpoint. Common situations where Cisco sees this are internal provider-to-provider, no patient involved, video consultations.

Jabber Guest
Cisco Jabber Guest is a consumer-to-business (C2B) solution that extends the reach of Cisco’s enterprise video to people outside of a corporate firewall who do not have devices registered with Cisco Unified Communications Manager. It provides a means for video to be integrated into a web page, iOS, or Android application.

Cisco sees the primary use cases of Jabber Guest being the web or mobile video client for patients and where an organization wants to fully leverage their current Cisco video infrastructure without many additional servers, licensing, or the need for professional services.

Pros:
- Chrome, IE, Firefox, and Safari support. All require a browser plug-in.
- iOS and Android mobile support.
• Registration of an account/phone on CUCM is not required.
• Connectivity and interoperability with all other Cisco video endpoints.

Cons:
• You can only call out. You cannot call a Jabber Guest endpoint from another Cisco video endpoint.
• Video only. No chat, screen mirroring, or voice only (without video).
• No remote Pan-Tilt-Zoom control of the other connected endpoint.

Common Use Cases:
• Integration into a web portal or mobile application to serve as the patient-facing endpoint.
• With the use of Cisco Extended Care or other 3rd party workflow software (release pending), integration into the telehealth workflow software’s web portal/interface.
• With the use of Cisco Extended Care, integration into EMR’s web or mobile applications (release pending).

Remote Expert Mobile
Cisco Remote Expert Mobile integrates video with business and mobile applications so patients can initiate face-to-face interactions with care providers and agents in the contact center. It allows video, voice, chat, screen mirroring, and remote annotation functionality to be integrated into a web page, iOS, or Android application.

Cisco sees the primary use cases of Remote Expert Mobile being the web or mobile video client for patients. It is a great fit where one wants and has the budget for a feature rich and heavily customizable client, or where additional functionality of voice, chat, screen mirroring, and remote annotation is desired. Loosely related to telehealth conversations, Remote Expert Mobile also has the advantage of tight integration into Cisco Contact Center, enabling skill based routing of incoming calls and an OmniChannel experience for customers/patients.

Pros:
• WebRTC, so no browser plug-in required for WebRTC compatible browsers
• iOS and Android mobile support
• Feature rich
• Highly customizable

Cons:
• You can only call out. You cannot call a Remote Expert Mobile endpoint from another Cisco video endpoint.
• Additional server-side components are required.

Common Use Cases:
• Integration into a web portal or mobile application to serve as the patient-facing endpoint.
• With the use of Cisco Extended Care or other third party workflow software (release pending), integration into the telehealth workflow software web portal/interface.
• With the use of Cisco Extended Care, integration into EMR web or mobile applications (release pending).
• Enabling an OmniChannel experience with integration into Cisco Contact Center.

4.4.2 Physical Endpoints
At a high level, an endpoint consists of a screen, microphone, speakers, and one or more video and audio processing devices called codecs.


Of these endpoints, Cisco most commonly sees desktop personal systems DX70, DX80, EX60 and EX90, and the mobile video carts manufactured by Cisco partners deployed for a wide variety of telehealth use cases. Cisco also sees the rare use of multipurpose systems, the Cisco MX line, but generally do not see these purchased solely for telemedicine but rather used
when the hospital wants to leverage their existing endpoint investment or has plans to have the endpoint for other traditional TelePresence needs.

**Pros:**
- The best video quality
- Additional TelePresence feature sets like integrated bridging and remote pan-tilt-zoom control
- Ability to receive a call as well as call out

**Cons:**
- Relative lack of mobility

**Common Use Cases:**
- Generally Cisco will see the DX and EX series used as the provider side endpoint for a multitude of use cases.
- Mobile carts are a great format for bringing a high quality video experience to the patient’s bedside.
  - Note that many of the third party carts have inputs for medical devices and the output from the device can be sent over the video channel.

### 4.5. Workflow Software

As noted in the [Architecture Components](#) section, many telehealth use cases can be solved with just connecting one Cisco endpoint to another similar to what would be done in traditional TelePresence scenarios. However there are several use cases where you may need additional workflow software. In these use cases additional functionality like integrating billing, virtual queuing, EMR integration, e-prescriptions, skill based routing, and so on is required.

#### 4.5.1 Functions of Workflow Software

In this section the paper will detail some of what Cisco sees as the important subset of functions that a workflow software can bring to the table and a high level overview on what purpose each function serves. The goal of this is for you to be able to have a consultative conversation with the project leaders as well as identify needs and requirements where you will need to add a workflow software component to the telehealth design. It should be noted though that instead of using dedicated telehealth workflow software many of these components can be accomplished by other manual or automated means that the hospital has in place. Therefore, when consulting consider these questions:

1) For your use cases do you need this functionality?
2) Do you have any mechanisms currently in place providing this functionality and if so do you plan on continuing to use these mechanisms going forward?
3) If set of functionality identified will be a net new addition, then identify the best workflow software system to meet those needs and allow for growth into future needs in line with the hospital’s strategic direction.

Also, when thinking of these functions you will find that a majority are really electronic means that mirror the functions and needs that would occur in a traditional brick and mortar environment.

- **Visit Info: Reason for Visit** – Allow the person who is requesting the consultation, whether that is a patient or internal provider, to put in their symptoms, needs, and/or what expertise they are looking for. This can be used to help route the request to the most skilled provider (using skill based routing), to trigger other workflow steps like a specific questionnaire to be completed, or to simply give information to the answering provider to know what the request is about.
- **Visit Info: Health Survey/Questionnaire** – The ability, commonly for the patient, to fill out a health questionnaire form similar to one that you would fill out in the physician’s office.
- **Provider Availability** – This can break down into two components. The first is a calendaring system to input what providers are assigned to cover incoming calls for that specialty and at that time, and you can think of this as an on-call calendar. The second part of this is for those providers that are assigned, who are currently available as determined by not currently being on another call or via some sort of integrated availability presence functionality.
- **Skill Based Routing** – Using Reason for Visit combined with Provider Availability, route the request to the most skilled and available provider.
- **Patient Queue** – The ability that when a patient initiates the session from their side that they are placed in a virtual queue pending the provider to join the session. This is done as opposed to directly calling the provider. For a brick
and mortar analogy, think of an urgent care clinic where the “queue” is the room you are waiting in and the nurse and physician come in and out of that room as opposed to you walking directly up to the physician and initiating the visit.

- **Notification of Waiting Patient** – When a patient is in that virtual queue how is the provider notified that they have a waiting patient? Many systems will send a text message or phone call informing a designated person that the patient is in queue.
- **Scheduling and Calendaring** – The ability for a patient to either request a time window when they would like to have an appointment or ideally just pick a specific time in the future. This functionality would not necessarily apply to situations where the consultation is requested and initiated immediately. If a window of time is requested then the workflow needs to be determined for who sees that request and schedules the specific time during that window. Once the specific time is determined, either automatically or manually, it needs to be determined how the provider will see that request (calendaring) and how they are notified that they have a new appointment. Also it should be determined if there any other parties that need to approve a request prior to it being made official.
- **Patient History** – Directly though the workflow software does the provider need to be able to see the patient’s medical history? Note that the key functionality distinction here is do they have to see it through the telehealth workflow software itself or will they view it directly though the EMR interface that they may have running in parallel.
- **Registration for New Patients** – For some use cases the hospital is targeting the program to get new patients into their health system, and if this is the case what will the process be to have the patient create a user ID/password and provide the information that the hospital requires for registering a new patient in their system?
- **Medical Device Integration** – Does the use case require the transmission of data from medical devices such as stethoscopes or exam cameras over the video channel? Then, related to the workflow software itself does any data or pictures from these devices need to be entered into the workflow software? A point of clarification here is that you should separate out the use and transmission of any audio or video from devices from the entry of data that these devices create. For example, it is a completely different set of requirements to say that there is a need to use an exam camera to transmit the look of a rash over the existing video session rather than saying pictures from this camera need to be stored in the workflow software. Then, if those images are stored there is a key difference between the functionality to manually upload these pictures as opposed to having them automatically entered in the system when they are taken.
- **Document Share** – The capability for a provider or patient to be able to bring up a document, medical image, or perhaps application such as an EMR and be able to share that material or their screen over the session.
- **Educational Videos** – The capability for educational videos to either be directly stored in the system or the system’s ability to link to a video share. Then, a provider can assign videos for the patient to watch, the patient has remote access to those videos, and watching of those videos is logged for compliance.
- **EMR Integration** – The ability to enter data measurement and findings data directly in the workflow software and have that data automatically sent to the EMR at the conclusion of the session likely though HL7 integration.
- **Patient Viewing Results** – The ability for the patient to receive and/or be able to view online the results of their session. Cisco will often see this done using the existing functionality of the EMR instead of adding on additional functionality and what is often a separate database with the telehealth software.
- **Secure Messaging** – The ability to send a HIPAA compliant secure message between providers, from the provider to the patient, or patient to provider.
- **E-Prescribing** – The ability for the provider to enter an electronic medication prescription and have it sent to one of many partnering pharmacies.
- **Billing** – The ability for the patient to pay for the service prior to that service actually taking place. This may be paying a co-pay in the event that the patient is covered by insurance or could be paying for the entire cost of the visit in the case of high-deductible insurance plans or could be a completely out-of-pocket payment. The part of taking the payment can often be the easier part of this functionality and what may be more technically complicated is how do you determine how much to charge? Things that can factor into the amount of the charge are the type of visit, the type of insurance the patient has, and any promotions the hospital is putting on.

### 4.6. Security

From a security perspective, there are many considerations when implementing a Telehealth solution. Many of these considerations are best practice for security, but some are often overlooked.
**Encryption in Signaling and in Transit**


For supported Cisco Unified Communications devices, signaling and media can be encrypted to prevent eavesdropping and reconnaissance attacks on active calls and during call establishment. The protocols and mechanisms used to provide secure communications and signaling within Unified Communications deployments include the following:

- Transport Layer Security (TLS) used for encrypting signaling traffic,
- Secure Real-Time Transport Protocol (SRTP) and Secure Real-Time Transport Control Protocol (SRTCP), used for encrypting media,
- Datagram Transport Layer Security (DTLS) Secure Real-Time Transport Protocol (SRTP), used for SRTP master key negotiation and/or exchange,
- Digital Certificates,
- Certificate Authority Proxy Function (CAPF),
- The Certificate Trust List (CTL).

Cisco Unified CM, Cisco TelePresence System (CTS), and Cisco Video Communication Servers (VCS) support secure signaling using TLS for SIP. In implementations where a SIP trunk is used for integrating Unified CM, VCS, and CTS, end-to-end signaling encryption of SIP protocol is supported using TLS.

**Perimeter**

Depending upon the architecture that is selected, you have to look closely at any Internet facing devices including those in the DMZ. You must consider that unauthenticated devices will be connecting to the device and possibly to the internal network. Placing a control in front of these devices, such as Web Application Firewall (WAF), is critical. This will help control the traffic coming into the device, helping to reduce connections with malicious intent, such as DDoS, Cross Site Scripting/Forgery Requests, and possibly even SQL Injection and others depending upon what resides on that server. Ensuring the firewall, behind which this device resides, has a tightly controlled rule set only allowing the wanted protocols and communications through is also imperative.

**Traffic Profiling**

Adding in application control and malware/anti-virus scanning to help eliminate malicious traffic is also very important. Cisco NGFW, ASA with FirePower will help here.

**Segmentation**

In order to isolate traffic streams and data stores an organization must consider network segmentation. While an in depth discussion around this is beyond the scope of this paper, here are some considerations:

- Will any data traverse from the telehealth portal or session to the EMR or file storage system? This data is inclusive of, but not limited to, audio and video transmissions, chat/text notes, and information collected from medical monitoring devices.
  - Proper access control lists (ACL’s), firewall rules, and application control to limit both devices and individuals from unwanted access.
  - Digitally sign, hash, and encrypt the data to validate the integrity and protect the confidentiality of the information.
- Where will associated systems reside; Trusted network, DMZ or public?
  - Which hops of traffic need to be encrypted?
  - What type of encryption do you need to implement? HTTPS, SSH/TLS, file level.
  - Will you need to inspect this traffic (i.e. Will it contain files/documents that could be infected)?
    - Where will the traffic be decrypted and should it be re-encrypted after inspection?
- QoS can be implemented to ensure that telehealth sessions receive guaranteed bandwidth to significantly reduce jitters and dropouts. This is particularly effective on a dedicated LAN/vLAN.
Cisco servers, network equipment and security devices all support the encryption of data in motion and network segmentation.

**Authentication and Authorization**
In order to authenticate and properly identify users, using a portal with multi factor authentication would be helpful. In addition to a username and complex password, a One Time Password (OTP) could be used. This OTP could be sent to the user’s phone via SMS or e-mail address on file, or in certain circumstances via a voice call. Although more expensive, issuing a certificate could also be an option for those regularly using a specific device. Having a defined user in the portal and utilizing an OTP can help reduce the chances of charting in the wrong medical record, unwittingly disseminating PHI to the wrong patient, and increase the challenges of hackers gaining unwanted access.

One way to really control access would be to embed the video, chat, and/or voice communication directly into an authenticated portal. Having the WAF and an OTP would bring enhanced security and identification.

**Data Protection**
Not only should data in motion be protected, but if there will be any data stored outside of the EMR it should also be encrypted. This includes files, videos, audio and messaging, and both e-mail and text messages. Regardless if this data is stored in the cloud or on the trusted network it represents an increased risk. While on the topic of data storage, you should also address back-ups which need to be controlled even more carefully because if someone does gain access to this static data, they can take their time to brute force decrypt. Back-ups should be encrypted as a whole, on top of the data inside being encrypted; they should reside behind tightly controlled firewalls which only allow access to a very limited set of users and devices. Additionally, any activity should be logged and alerted on for unusual activity immediately. Logging and SIEM will be discussed below.

**PCI**
For an organization accepting credit card payment via the web for Telehealth services, the recommendation is to use a third party re-direct to avoid PCI and/or reduce scope as much as possible. The PCI rules require that any device connected to the same network segment be considered in scope, making even more of a case for an appropriately segmented network. If payment is going to be taken directly from the web portal via an embedded form or iFrame, monitoring will also be required to adhere to PCI-DSS. The Acquiring Bank will help to determine how this will affect your PCI level and if you need to fill out a SAQ or ROC.

**Monitoring**
If properly configured and implemented, all of the security controls discussed will greatly reduce the risk of data leakage and non-compliance but there is one critical piece that is often overlooked despite being required by nearly all compliance and regulatory frameworks and that is monitoring. The utilization of a SIEM or logging tool to aggregate and correlate the logs is imperative. Programming in well thought out and specific Use Cases to generate the appropriate alerts and then sending those alerts to properly trained staff who can quickly weed out the noise and react to important issues in a timely fashion is how risk is reduced. When selecting a SIEM and/or MSS vendor, one must have a clear picture of the architecture, how it integrates, and what devices are important to monitor. Knowing what types of logs or data is available from those devices (SYSLog, SNMP, NetFlow, etc.) will help in the selection of technology and service providers. Not only is this required to meet HIPAA and PCI compliance but also it is unmistakably a security best practice.

**Additional Considerations**
Some additional considerations but not necessarily built into the Telehealth architecture are how the following devices will be given access to your network and if you must have any controls.

- **End point protection:** Will your organization be allowing patient devices on anything other than a corporate network or be allowed to send files through the secure systems? If so, interrogating the devices to ensure they meet a standard of patching and AV/Anti-Malware protection may be desirable. A compensating control of having the gateway anti-virus/malware detection devices is appropriate, but it is critical for the data to be encrypted before it is scanned, then re-encrypted as it is sent on to its final destination.

- **Mobile endpoints access:** In addition to the end point protection comments above, one must consider the applications, rooted/jail broken status and lack of consistent AV/Anti-Malware protections available for these
devices. It is better to require these devices to sit on an isolated guest network and access the tools just as if they were at their home or alternate location.

- **Containerized sessions**: For some potentially high risk sessions or to address low bandwidth in remote locations, it may be prudent to allow someone to use a temporary container or VDI implementation. Once the session is complete, the container or VDI can be completely reset. With the low bandwidth client using a VDI session will only require a web representation of the session thus reducing the bandwidth utilization.

- **Secure chat/text messaging**: If out of band communication is required for certain communications, such as a personal health monitor that may send data via SMS, it would be advisable to use a secure application for this.