

MSO's Health Over Cable

The Ways We Can Add Value

A Technical Paper prepared for SCTE/ISBE by

Mark Bugajski
SVP Advanced Technology
ARRIS
3871 Lakefield Dr.
Suwanee, GA 30024
mark.bugajski@arris.com

Paul Moroney
SVP Advanced Technology and GM Security Solutions
ARRIS
6450 Sequence Drive
San Diego, CA 92121
paul.moroney@arris.com

Table of Contents

Title	Page Number
Introduction _____	3
Bringing Health Monitoring Services Home via Cable Networks _____	3
Health, the IoT and Security _____	12
Secure Device Design _____	13
Conclusion _____	15
Abbreviations _____	16
Bibliography & References _____	16

List of Figures

Title	Page Number
Figure 1 - Global Aging Trends	3
Figure 2 - USA Aging Trends	4
Figure 3 - Connected Medical Devices and Associated Challenges	4
Figure 4 - Health over Internet Challenges	5
Figure 5 - Health over Internet Required Measurement Steps	6
Figure 6 - Health over Internet Associated Risks	7
Figure 7 - Health over Cable Advantages	7
Figure 8 - Health over Cable User Experience	8
Figure 9 - Health over Cable and itUser Experience	9
Figure 10 - Health over Cable User Experience	9
Figure 11 - Health over Cable User Family Portal	10
Figure 12 - Health over Cable Individual User Portal	10
Figure 13 - Health over Cable VoD Experience	11

Introduction

Over the next 35 years, there will be a massive increase in the aging population that will require health care, despite scarcer human resources to provide that care. The Internet of Things (IoT) aims to connect medical devices to service providers and create The Internet of Health Things (IoHT). By transforming raw data into actionable information and communicating that information to everyday objects, machines, and people, the IoHT is becoming a vital tool to the healthcare industry. Although the IoHT promises to significantly lower the costs of healthcare to the aging populations of developed countries, the current Internet of Health Things are Over-the-Top (OTT) based, highly fragmented, and challenging for the average patient or consumer to use. Cable operators are in an advantageous position to partner with caregiving providers to create managed networks, use set-top boxes (STBs) as service portals, use STBs as medical devices with a built-in Bluetooth Low Energy (BLE) interface and utilize condition-specific Video on Demand (VoD). Most importantly, cable operators are able to provide a secure cable network, ensuring that a patient maintains their privacy.

Bringing Health Monitoring Services Home via Cable Networks

As is, modern nations will not be able to sustain the current level of care needed for baby-boomers and generations beyond them. In 2015, just 2.7 % of the world’s population was over the age of 70, roughly 190 million people (as seen in Figure 1). By 2050, the percent of people over the age of 70 is expected to rise to 6% of the world’s population (as seen in Figure 1).

Data source for Figure 1 and Figure 2: (www.populationpyramid.net)

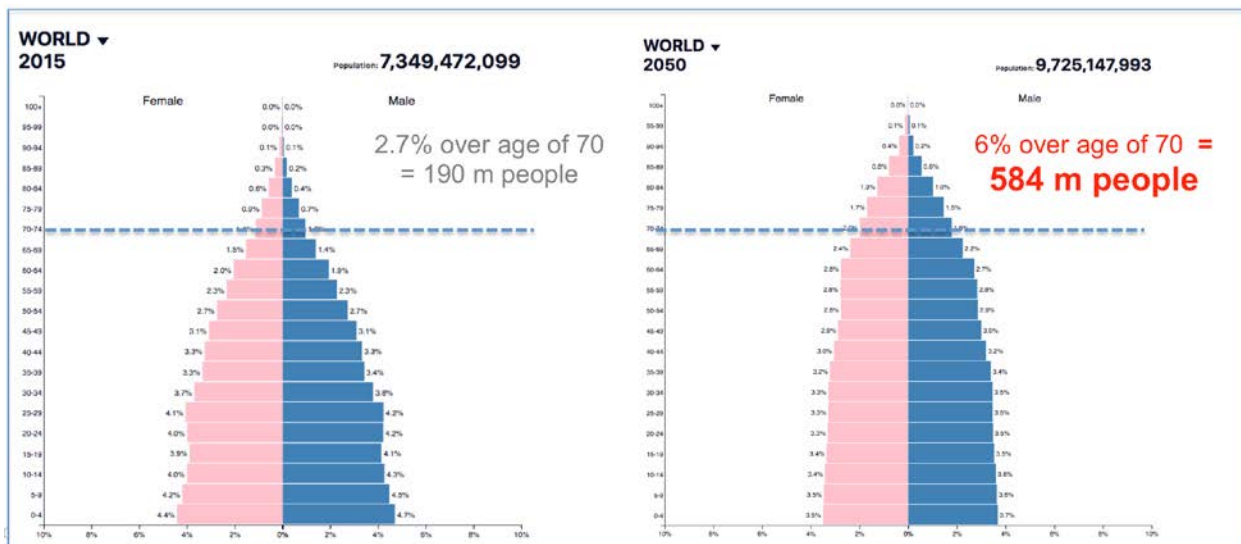


Figure 1 - Global Aging Trends

In the United States alone, 4.5% of the population, or 14 million people, were above the age of 70 in 2015 (Figure 2). This number is expected to rise to 32 million or 8.2% of the population by 2050 (Figure 2).

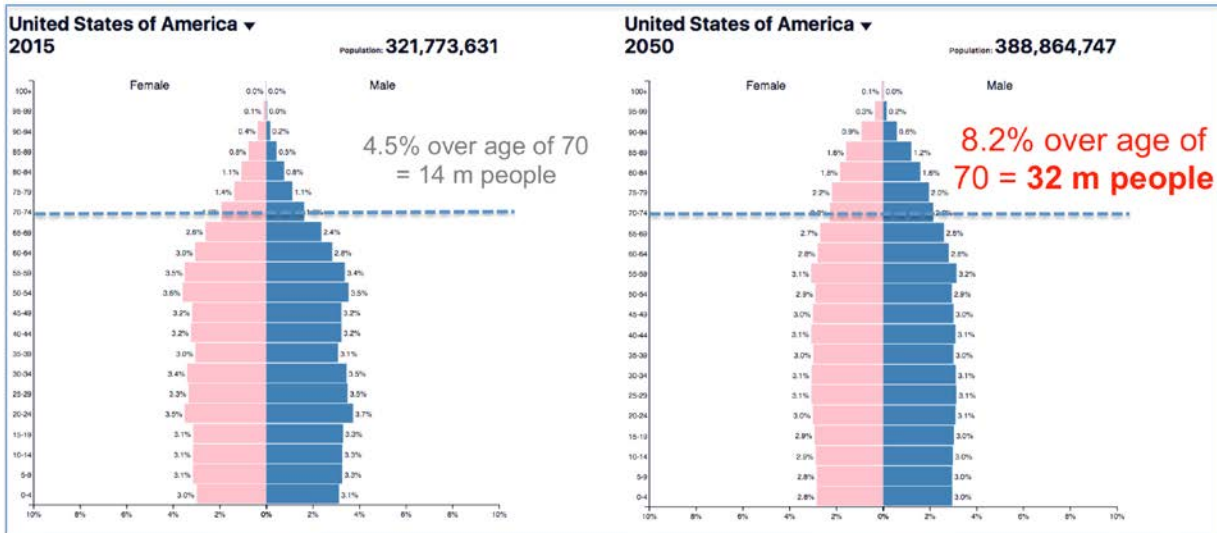


Figure 2 - USA Aging Trends

To address the care to the aging population problem, there has been a great deal of technological innovation aimed at producing IoHT devices that will offset the associated costs.

Currently, there is much work on miniaturization, portability, and significant cost reduction for IoHT devices that can do various things like monitor human vital signs and track the number of steps taken during the day using OTT mobiles and various wrist bands. Many health and wellness monitoring devices are already widely available in retail as seen in Figure 3.

Able to Remotely Monitor Vital Signs due to Standards Based Connectivity

- Connected Thermometer
- Alarm Button
- Motion Detector
- Weight Scale
- Pulse and Oxygen Level Meter
- Glucose Meter
- Breathalyser
- Pill Dispenser and Use Monitor
- Fitness Tracker
- High Definition Webcam
- more to come

The challenges:

- Separate apps for each device
- Connecting the caregiver
- Creating manageable and easy to understand regimes
- Enforcing the compliance
- Analyzing the data
- Following up with the patient
- OTT connections

Figure 3 - Connected Medical Devices and Associated Challenges

- BLE Connected Thermometers use wireless Bluetooth to send data from temperature sensors to smart phones and tablets, making the data easier to understand and send to relevant healthcare providers

- ZigBee Alarm Buttons allow users who have fallen, are having an acute medical problem, or are under threat of fire or burglary to activate wireless alarms and panic buttons to alert monitoring personnel
- ZigBee Motion Detectors trigger lights to illuminate darkened hallways or doorways and to turn on children’s nightlights. They also send text and e-mail alerts when motion is detected in empty houses, ensuring safety and security
- BLE Connected Weight Scales allow users to send their weight and BMI data into relevant apps that track health and dieting, while BLE Pulse and Oxygen Level Meters measure and wirelessly store blood oxygen levels, heart rates, and perfusion indexes
- BLE Connected Breathalyzers send blood alcohol levels to smartphones, and BLE Glucose Meters monitor glucose activity in real time, sending high and low alerts and alarms, and sharing data with selected followers
- Most popular, perhaps, are BT Fitness trackers which track, calories burned, steps taken, stairs climbed, and more

Though these devices are available and widely utilized, there are certain challenges in the existing technology as illustrated on Fig. 4, including the app diversity, connection to the caregiver, manageable and easy to understand regimes, compliance enforcement, data analysis, and follow-up with patients.

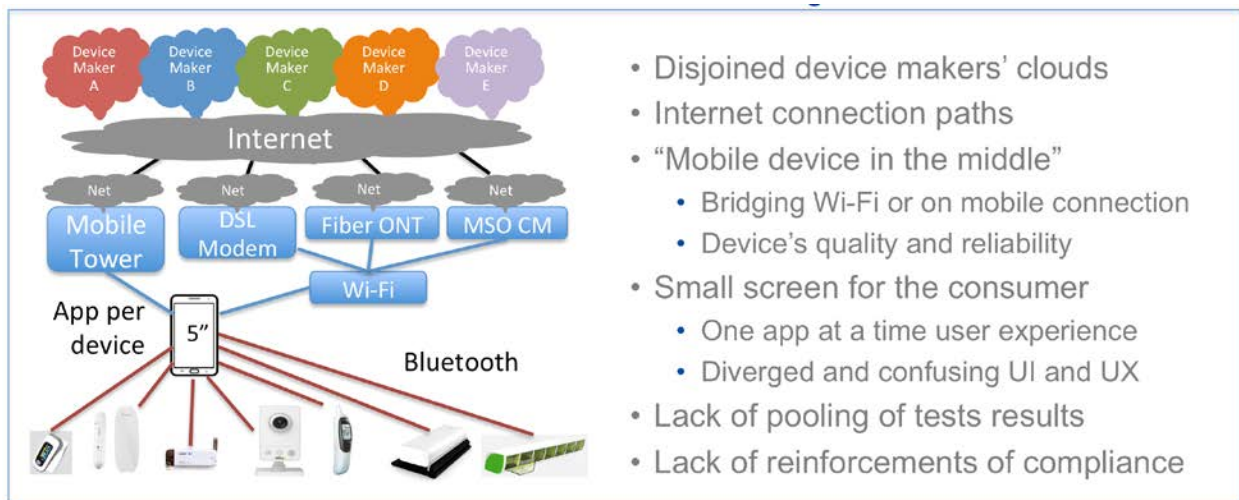


Figure 4 - Health over Internet Challenges

Furthermore, there are additional challenges in regards to the OTT connections. These include disjoined device makers’ clouds, different Internet connection paths to consumers, reliance on home Wi-Fi or on mobile connections, and dependence on mobile device’s quality and reliability. A too-small screen for the consumer, one app at a time user experience, diverged and confusing UI and UX, lack of pooling of tests and their results, and lack of reinforcements of regime compliance provide addition challenges to connections.

The current Health over Internet (OTT) method of communication with monitoring devices includes connection to the home gateway plus Wi-Fi connection to mobile devices. For example, smart phones and

tablets use Bluetooth to link to the point-of-use device like a thermometer, blood pressure cuff, pulse and oxygen level meters, scales, or other apparatus. Currently, the Wi-Fi and Bluetooth connections are not monitored by the service providers for quality and reliability. That quality and reliability of the measurement procedure depends upon several factors many of which are often outside the monitored person's or the patient's control. The required steps are shown in Figure 5.



Figure 5 - Health over Internet Required Measurement Steps

The lean-forward consumer experience requires the patient or care receiver to go through required steps. Initially, the monitored person must remember to take their measurements. For the purpose of this technical paper, “measurements” can be any information required for the health care application including: temperature, blood pressure, blood sugar reading, whether a scheduled medicine was taken, etc. The mobile device must not only be turned on, it also needs to be reliably connected to a Wi-Fi network. The battery inside the mobile device must have enough of a charge or have a connection to a power source. The appropriate app must then be found and launched by the patient. Usually, several on-screen navigational steps need to be undertaken to get to the monitoring device control. The monitoring device needs to be connected to the mobile device's Bluetooth. Only then can the test be initiated. After the test is complete, the results can be uploaded to the service provider's cloud.

Given all these steps, the current system of operation creates many points for error and failure as illustrated on Figure 6. Some of these steps are often difficult for the monitored person or patient to remember and correctly sequence as they interacts with the system. More importantly, the patient may not even remember to take the measurements in the first place. If the mobile device is misplaced or has a poor or intermittent Wi-Fi connectivity, then the measurement may fail to record or cut off early. The battery may drain, causing difficulty, or the device may go to sleep too early and interfere with the measurement taking. The Bluetooth radio may be disabled to save battery. The device may also have intermittent Bluetooth connection or drop the Bluetooth link altogether.

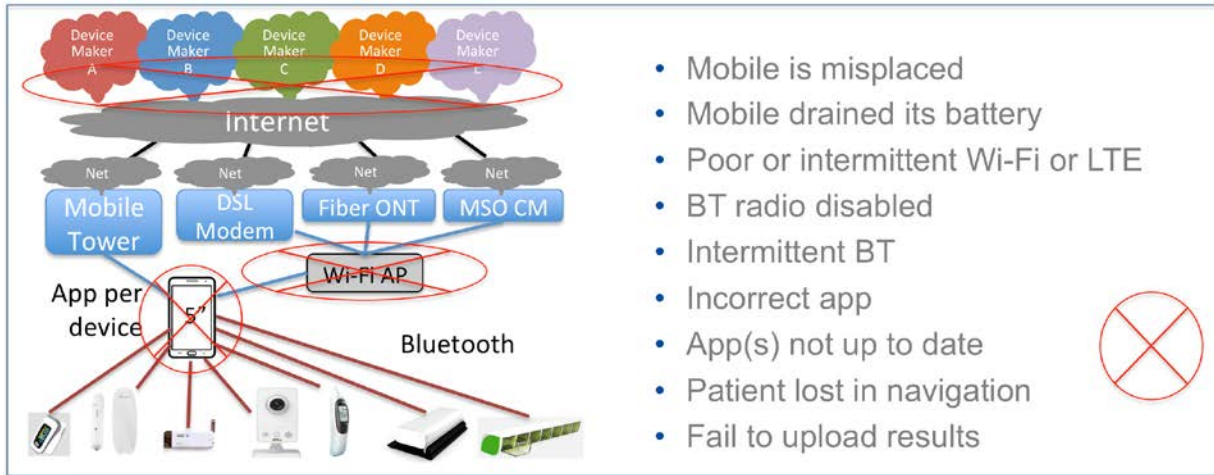


Figure 6 - Health over Internet Associated Risks

The incorrect app may start or the patient may start the incorrect app, and the patient may be very confused with the navigational steps. Finally, due to a variety of reasons, the device may fail to upload the test results.

In contrast, when a smart MSO set-top device with a built-in BLE interface is used to connect to the monitoring devices over a private MSO network, a much simpler and intuitively more reliable architecture shown on Figure 7 is being created. We can call it a **Health over Cable (HoC) System**. It consists of a cable operator owned set-top box (STB) to connect to all home medical devices over a totally private Intranet. It is assumed that the MSO partners with a healthcare or monitoring care services provider will connect in the MSO cloud.

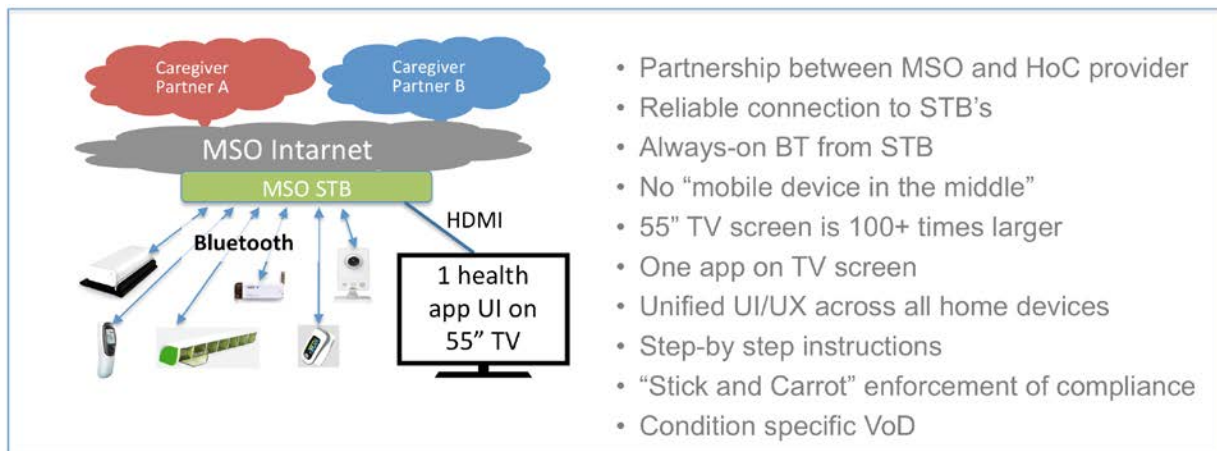


Figure 7 - Health over Cable Advantages

Cable operators are in a unique position to provide improvements in these areas. In order to offload hospital beds and provide real care to non-critical patients, cable operators could make the developments and take steps needed to provide beneficial solutions to their subscribers. The monitoring and care-giving portal in these healthcare devices must be extremely reliable and easy to interact with. Even people with a

limited understanding of technology, such as the elderly or mentally impaired, need to be able to understand and operate the simple interactive interface.

The same BLE fitted STB drives a large TV screen to become a portal to the patient. The patient interacts with the system using voice enabled remote or several buttons on such. The connection to the STB is wired and as such is very reliable. The BLE radio in the STB is “always-on” powered by the same power supply as the STB. There no additional wireless or mobile Wi-Fi or LTE connection required, because the device in the middle as it has been eliminated from the HoC architecture.

A large TV screen, 100 times larger than mobile device’s screen is used to interact with the patient. There is no need to touch any screens. One application replaces individual, per-device mobile apps. It features very simple User Interface and common experience across all medical devices. Step-by-step instructions are available with a single click of a remote’s button. The MSO can participate in the compliance enforcing features of the HoC system by motivating by manipulating video playout and awarding with VoD assets. On the education side, the MSO can make condition and life style specific content playable from the same app.

This architecture creates a comfortable lean-back experience for the patient. Instead of relying on an own individual’s memory, on-screen notifications remind and/or alert the patient to take the measurements. The HoC user experience is illustrated on Figure 8 with a number of simple steps needed to interact with the system.

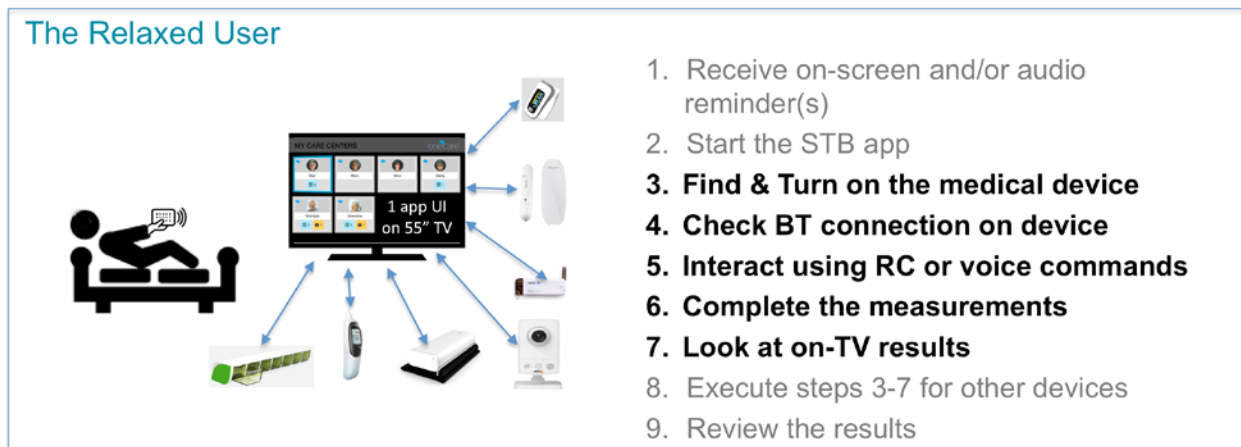


Figure 8 - Health over Cable User Experience

The on-screen notifications are being forced by an always-connected cloud. The patient does not have to worry or be confused about the order of steps because on-screen instructions direct and instruct the patient to correctly start and use the monitoring device. Prior to taking the measurements, the Bluetooth connection is automatically enabled. This allows for a quick connection to the device. Visual and audio prompts then help the patient take the measurements correctly.

The possible problems with HoC user experience are illustrated on Figure 9. The removal of a mobile phone from the connection to the patient makes this solution inherently more robust and easier to use. The same set of devices can be operated from a single TV screen using a remote or own voice to navigate.

The Relaxed User

Possible failures

- STB Remote is misplaced
- User failed to complete the measurements and will be notified of it (or TV programming will not resume)

Figure 9 - Health over Cable and itUser Experience

Another HoC user experience (UX) option stops TV programming altogether and notifies the patient to take their measurements. In order not to miss any of the programming, the TV program is then recorded to a local or cloud-based DVR (as shown on the screenshot of the TV screen on Figure 10). After the alert, the patient is taken to the device control screen and STB will wait for their input (voice control or a click on the remote) to start the measurement.

- Care recipients and their family can be alerted by the on-screen and audio notifications from the HoC providers
- TV stops playing the content if measurements are not taken
- The TV screen will assist with measurements

Figure 10 - Health over Cable User Experience

The measurement will be shown and immediately uploaded to the cloud. Then, if needed, TV programming will resume and/or a reward can be awarded to the patient for complying with the program. The reward could be in a form of free VoD movie or a temporary access to premium channels.

The TV screen, which is powered by the always-on STB and voice-enabled remote, are in exactly the right place to deliver the condition-specific VoD content, educate the patient, connect with their nurse and doctor, and bridge the healthcare community.

There are a significant number of advantages to using the patient’s TV screen as a portal that brings connected health and wellness to the care-receiving household:

- A TV with an average screen size of 55 inches is more than 100 times larger than a mobile device’s screen, which has an average screen size of 5.5 inches
- Due to the TV’s larger size screen, there is real estate for much larger user interface, which will help enable the patient or care receiver to clearly see the information on a big screen as illustrated on Figure 11
- The patient’s or care receiver’s family members or household members can be alerted by the on-screen and audio notifications. Even from a distance, the large screen allows family members and visiting caregivers to view the information and be attuned to the care being administered as illustrated on Figure 12

- 55” TV screen is more than 100 times larger than 5.5” of a large mobile phone
- The patients, family members, visiting care givers can clearly see the information, even from a distance
- Local or remote family members can be integrated on one portal

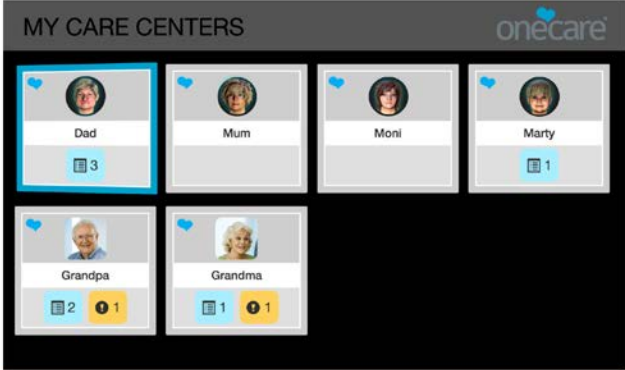


Figure 11 - Health over Cable User Family Portal

These notifications from the service providers help family or household members assist the monitored person in measurement taking activities. Furthermore, with the care recipient’s consent, the care-giving service provider can deliver condition-specific on-demand video content to the TV screen.

- To-do tasks can be viewed by the patient or be shared with other HoC subscribers
- The care-giving MSO partner hosts this portal
- Person’s avatars can be created and updated from uploaded photos

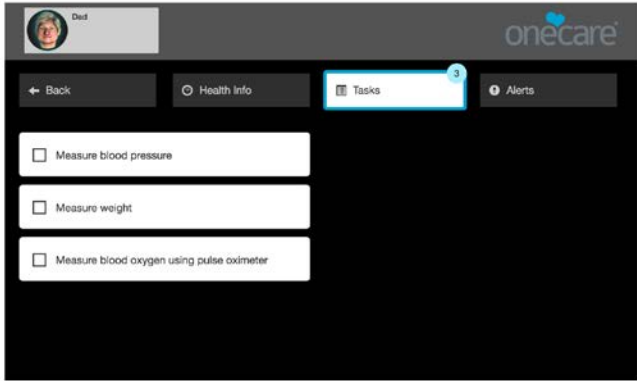


Figure 12 - Health over Cable Individual User Portal

The condition-specific content can be of a linear, lean-back nature. It can also be interactive to ensure that the patient pays attention to it and help them to remember the do's and don'ts associated with the condition they have and the measurement taking activities. The condition-specific content could also be expanded to recommend diets, exercises, and changes to one's lifestyle and behavior. Individual monitoring tasks can be viewed by the patient only or can be shared with other HoC service providers.

Also, the service provide could set up a content exchange portal for patients with similar conditions. Patients with the same or similar conditions can browse through the portal, select it for viewing, and interact with it in many ways as illustrated on Figure 13. Other patients can share links to any relevant content that may be of interest to the patient. The care-giving MSO partner hosts the portal, and the patient's avatar can be created and updated from uploaded photos.

On-Screen HoC VoD Experience

- The care-giving service provider can deliver condition-specific, on-demand video content to the TV screen
- The content can be of a linear, lean-back nature but it can also be interactive to ensure that the patient pays attention to it .
- It can be expanded into recommending diets, exercises and changes to one's lifestyles and behaviours
- The service provider can setup a content exchange portal for the patients with similar conditions

Figure 13 - Health over Cable VoD Experience

Cable service providers and application developers will find that there are many significant advantages to using the STB as a service portal. STBs are always connected. Connection to the Cloud is under total control of the service providers. This kind of connection to the Cloud is more reliable than a connection to any other device, and it is monitored and managed 24/7 each and every day. The STB is less likely to be unplugged from the wall, and unlike mobile devices, STBs are always connected to the Internet, even when they are not used. STBs do not need local health-care application storage. Rather, they only need an engine to render a cloud-based app. STB variety is limited, and the number of apps used in manageable. With STB, there is no need to support generations of mobile devices, and there is no need to support generations of OSs.

Cable providers are also able to offer improvements by ensuring reliable connections between the care-giving cloud and the patients. The cable modem termination system (CMTS), the home gateway, and all the connections between it and the medical devices need to be rock solid. Cable service providers have what it takes to create and maintain strong connectivity, because they have already invested heavily in very reliable networks. These networks are fiber-deep, with diverse routing and powering infrastructure. This infrastructure is able to be baked-up by alternative sources of energy. The central office DOCSIS systems have been designed and built by companies with deep roots in telecommunications. Therefore, they feature very high uptime specifications.

Modern STBs have built-in DOCSIS Cable Modems that are separate from the Internet Cable Modem. STBs are being installed by the MSO technicians what guarantees their reliable connection. Cable companies have taken major chunks of broadband services away from Telcos. This did not happen by chance. It happened because of superior connectivity and speeds offered by cable companies. Cable Home Gateways undergo tough and comprehensive compatibility and reliability tests performed by independent parties prior to their deployment in the field. Some provide lifeline telephony services at par with legacy telco equipment. Some modern STBs already feature low-energy Bluetooth interfaces to connect the remote control. These can be compatible with the medical devices. New generations of STBs are being specified by the service providers and OTT companies, including Android TV require BLE interface.

Cable providers can consolidate the fragmented OTT apps from one-per-device and integrate them into an intuitive, easy to interact with web app that would be under the control of the service provider. The new app could use the entertainment content as a reward for good behavior, compliance with the monitoring regime, and the taking of medication.

Today's health monitoring system landscape is highly fragmented. Every manufacturing company wants consumers to use their individual apps. They argue their app layer security and look for future recurring subscription revenue. However, these apps do not allow for the creation of very useful if-this-than-that (IFTTT) sequences of events across multiple devices. They do not allow for the pooling of measurements into sessions that could be reminded of via notifications and automatically invoked for the consumer. Such a pooling would be very useful for patients, particularly for those patients who are being asked to do multiple tests and measurements in a continuous session.

STB portals, on the other hand, have ample TV screen space. This screen space could show, at the same time, multiple devices that need to be operated. It could guide the patient through any procedures in a step-by-step manner. The procedures might include anything from taking the patient's pills from the connected dispenser, to taking the patient's temperature, and to performing blood pressure measurement. The application could urge patients to get on a weight scale and instruct them to test pulse and oxygen levels.

A key advantage of having the connected health application on the cable service provider's STB is the ability to link the cable service provider's or patient's VoD system to the application. An innovative rewards system can be integrated with the app to offer rewards to those who comply with the regime they agree to follow. For example, a free movie could be granted to the patient or care receiver when they follow the schedule and report the measurements.

Health, the IoT and Security

There is little doubt that the emerging world of IoT devices specific to the HealthCare industry can provide extreme value in terms of controlling costs, access to health care, more accurate and current monitoring of treatment programs, and remote diagnostics. However, it is also critical to examine the risks that exist with these new devices.

At a minimum, the consumer data accessible through such IoHT devices should be considered extremely private, and fully protected under the federal HIPAA rules. The relevant data must be accessible only to the intended parties, and only for the intended uses. For example, blood pressure data must be accessible to the family physician or specialist, and only for the purposes of medical diagnostics. Even the proper doctor should not employ the data for any other purpose. Thus not only the device must understand the

proper connection for data transfer, but the processing software at the doctor's office must be designed for diagnostic uses alone, to the extent possible.

Secondly, malicious intent must be blocked to the maximum extent possible. Hacking to steal data is certainly not desired, but hacking that plants a virus and defeats the intent of the IoHT device could cause improper readings. Not only can normal data be changed to show abnormal readings, but abnormal readings might be blocked, disguising or delaying real medical needs and treatment. Health devices can be held hostage, in the sense that private data can be threatened with exposure unless some ransom is paid. For health devices intended to accept commands for remote treatment, the impact can be even more devastating, including improper dosages and even death. The need for security in all phases of the device design and usage cannot be understated.

Further, hacking should not be viewed as strictly a remote access concern, although that is the primary attack mechanism. It should also be extremely difficult to alter such a device physically, when an attacker has the opportunity for direct access to the device. This access would include factory access during the manufacturing process, warehousing access, shipping access including interception and replacement, and even access once a device has been installed in the home. Where a consumer's health is concerned, everything must be considered.

In addition to IoHT device security design having regulatory aspects (HIPAA) as well as a safety concerns (hacking), it is important to look at this as more than just "meeting requirements" and "preventing problems." Secure design of such devices can be a competitive advantage. This type of device and marketplace carries the very real opportunity for increased value for increased security. Most consumers can accept that health diagnostic and treatment is not an area to choose the lowest price; reputation based upon better security in design and in process can translate to better value and thus greater market share.

Secure Device Design

What are the general guidelines for designing health targeted IoT devices in a secure manner?

1. Application layer communication protocols and security algorithms defined by a reputable industry consortium, such as OCF [Open Connectivity Foundation]. Health diagnostics and treatment is no place for creativity in this domain. Protocols and algorithms must have survived the test of time, and been subject to broad scrutiny and analysis. A unique algorithm invented during the design process may seem to present advantages of various types, yet time and again such an approach has proven disastrous in the security field. The protocols defined for health environments will ensure that all private data never appears in transit in unencrypted (clear) form.
2. HIPAA rules also require that private data stored in the device and in the servers in the infrastructure medical systems must be encrypted.
3. The software that runs on such an IoHT device must be updatable in the field. The manufacturer has an on-going obligation to keep these devices up to date in terms of flaws discovered after shipment. Any such update scheme must be secure; as such schemes are not necessarily standardized, they must use industry accepted techniques, and be scrutinized for flaws during the design process. Further, solutions cannot be burdensome to the consumer. As an example, mailing a security update notice to the consumer, requesting that they take some obscure action involving pressing hidden reset buttons, and even worse, loading code manually, are not going to be acceptable ways to assure then on-going safety and protections assumed in these devices.

From a long term view, the responsibility for selling secure health industry IoT devices is not just about shipping working devices and updating them as needed. There is an entire lifecycle to consider. Any company that choose to exit the business, or drop a product line, still must commit to continuous update, or arrange for another company to “take over” that process. Further, when devices reach end-of-life, there needs to be some procedure for disposal, some proper handling recommendations, as private data may still reside in the device.

4. A unique identity is critical for each device. Most likely, it is a specific requirement of the industry protocols described in the first item above, and often in the networking layers below the application layer. Diagnosis and treatment are always specific to an individual, so the system approach must uniquely identify the device or devices in use by any specific individual. To achieve this, devices likely have factory identities installed by the manufacturer, which are used to bootstrap a process for installing application level identities relevant to the application ecosystem in use (again, for example, OCF).
5. Secure software design practices should be followed. Many scanning tools exist to discover vulnerabilities in software, and the use of one or more of these should be standard practice.
6. To minimize hacking, devices should include physical robustness protections. Devices should be difficult to disassemble, and once disassembled, critical data should not be exposed on easily accessible busses or circuit connections. Test modes should not exist that defeat any protections. Examples for some of these practices are described in NIST publication [FIPS levels] and in the example Robustness Rules of Appendix C of the DTLA License document. This last document comes from the content protection industry, which shares some of the same needs as the health industry.
7. In general, all aspects of the secure processing within the infrastructure and the device should be documented and reviewed. Security process checklists often assist, with entries for all aspects of what can be done to protect the integrity and privacy of health data and device secrets. Any audits and reviews of this type should be recorded, and made available as the need arises. If any industry validation group is created for assurance, the manufacturer should submit designs to that group, and market compliance to its requirements.

Some Security Specifics:

1. All software resident on the consumer device must be signed cryptographically, to ensure that a trusted party wrote the code that it executes. Most often, the cryptographic algorithm is RSA, although code signing with elliptic curve cryptography can also be done. Note that the trusted party creating and signing the code is likely to be the device manufacturer, and there are obligations to perform such signing operations very securely, never exposing the signing key.
2. Software must carry a version number, also signed or otherwise secured, so that any device can determine if it has up-to-date code. Any device that has software that is out of date would initiate a download of the update. Devices must be able to check to see if their software is current; if such check is unable to be performed, there may be an attack underway, and a proper response is required.
3. Signature checking in the device must be performed in such a way that it can be traced to a “hardware root of trust,” making it extremely difficult to circumvent the signature check process. Generally, this requires the device to have a single secure silicon device implementing a secure boot process at power up, which builds trust a layer at a time.
4. Each device should have a unique manufactured cryptographic identity, typically composed of an elliptic curve cryptographic key pair, and a certificate attesting to the authenticity of the public key of the pair. The certificate should originate from a trusted Certificate Authority, and the

private key of the pair should be protected within the IoT device so that its use is not exposed outside of the secure silicon device. This secure identity can anchor the download of application level secure identity information.

Once these requirements are fully appreciated and understood, it is easy to see why Cable Home Gateway devices are ideal IoHT “concentrators” or partners in the home solution for health applications. Cable gateways implement all of the secure design principles listed above, as they often include content protection as well as privacy features for their normal operation support. Their connection to the Internet and thus any health systems in the infrastructure is highly reliable and secured, and they often include home networking radios within the design, making them ideal for in home connectivity to various IoHT devices.

Further, such devices typically operate in a closed system, with signed code, secure boot, and well controlled access. Compared to today’s mobile devices, they represent a far more secure choice for IoHT functionality. It is far too easy to install applications on today’s mobile phones with their more open ecosystem that either steal data directly or allow hackers to gain access.

Conclusion

Soon, we will experience a wave of baby-boomers entering the phase of life in which they will need health care, and consequently, there will be an increase in the pressure on the global health systems. The Internet of Health Things (IoHT) is promising to significantly lower costs of moving health monitoring to the aging population’s homes by developing standards based devices that can be easily connected to the cloud.

Cable operators are in an advantageous position to partner with care-giving service providers to enable Health-over-Cable (HoC) offerings to the patients at their homes. Health/wellness monitoring devices can be connected via a managed network. Set-top boxes (STBs) can connect to the medical devices using built-in BLE interfaces. TV screens connected to STBs can act as HoC services portals. On-screen notification and reminders can force the patient to comply with the regime. Patients can be rewarded by MSO’s video offerings. Condition-specific V-D can be streamed to the patient’s homes. Most notably, this can all be accomplished in a secure and private cable network.

There are some important things to remember when offering improvements to the Internet of Health Thing. Security for all is paramount. First of all, the normal HIPAA level of privacy and protocol security would be designed into the system. Then, patients would have to be assured that malicious hacking of all types would be deterred. They would also have to be assured that a response to any detected incident would be immediate and swift. Their health security and privacy must be the most important factor in the creation of the system.

Cable operator equipment is the ideal place for true physical security and threat mitigation. Therefore, cable operators are ideally positioned to monitor and control these devices. After all, they have a long history and a lot of experience with video content protection, secure data delivery, and secure software updates.

Abbreviations

BLE	Bluetooth Low Energy
CMTS	Cable Modem Termination System
DOCSIS	Data Over Cable Service Interface Specification
HoC	Health over Cable
HoOTT	Health over OTT
Hz	hertz
IFTTT	if-this-than-that
IoHT	Internet of Health Things
IoT	Internet of Things
ISBE	International Society of Broadband Experts
MSO	multiple system operator
OS	Operating System
OTT	Over-the-Top
SCTE	Society of Cable Telecommunications Engineers
STB	Set-top Box
UX	user experience
VoD	Video on Demand

Bibliography & References

Population Pyramids of the World from 1950 to 2100, aging charts and stats:

<http://www.populationpyramid.net>

Digital Transmission Licensing Administrator (DTLA): <http://www.dtcp.com/agreements.aspx>

National Institute of Standards and Technology (NIST) publication [FIPS levels]:

<http://csrc.nist.gov/groups/STM/cmvp/standards.html>

Open Connectivity Foundation: <https://openconnectivity.org/>

The Office of the National Coordinator for Health Information Technology, a division of the U.S.

Department of Health and Human Services: HealthIT.gov