KEYFACTOR

SECURE EVERY DIGITAL IDENTITY

WHITE PAPER

Secure IoMT: Enabling the Safe Delivery of Virtual Healthcare

Table of Contents

OVERVIEW 3

INNOVATIONS DRIVING VIRTUAL HEALTHCARE 4

Emerging Technologies 4

Internet of Medical Things (IoMT) 6

INNOVATING WHILE BUILDING TRUST 7

Securing the New Perioperative Loop 8

Conclusion 10

Overview

INTRODUCTION

Throughout most of the late 20th century, if you woke up and didn't feel well, you would call your family doctor, explain your symptoms, and if necessary, make an appointment to see your physician in his/her office. Appropriate tests would be prescribed and results analyzed. Depending upon the diagnosis, a hospital stay might be part of the process. You would be admitted, moved through a surgical intervention, spend time in recovery via a surgical ward, and then head home to heal. This "perioperative loop" scenario was played out, each and every day, all over the globe.

FORCES TRANSFORMING HEALTHCARE

While effective, this lengthy cycle of care was and remains expensive. Between staffing, general administration and operational expenditures, the cost of serving a patient end-to-end is astronomical. As value-based care becomes more and more prevalent, healthcare delivery organizations (HDOs) are looking to transform this model with goals of reducing costs, optimizing patient outcomes, and driving better financial performance.

A core component of this transformation is the shift to telemedicine or virtual healthcare. Advances in medical technology combined with the power of digital connectivity is allowing the doctor/patient interaction within a perioperative environment to become a partnership. For HDOs and insurance providers, reducing the time a patient is in a facility makes sense because operational costs go down. If you're an EHR (Electronic Health Record) provider or OEM (medical device manufacturer), you're thinking about how your technology should complement the HDO to help them meet their goals.

For patients, becoming an active participant in the process rather than an "observer" provides control and drives accountability. By taking ownership of their healthcare, they are accepting greater responsibility for their off-site recovery. These changes are momentous – the industry is literally breaking down walls of how healthcare is administered and delivered.

This transition is facilitated by healthcare's ability to adopt and harness the power of widely accepted consumer technologies. These technologies are blurring the lines between traditional medical device manufacturers and the brands that consumers know very well.

These converging forces have shredded the myth of a hospital being the only facility that can deliver care. Time will tell how the role of the HDO shifts within this new ecosystem. But HDOs must make decisions today about how to invest in these technologies to stay relevant. As this transformation evolves, we will see technologies, devices, processes, and skillsets develop that align to the industry's goals.

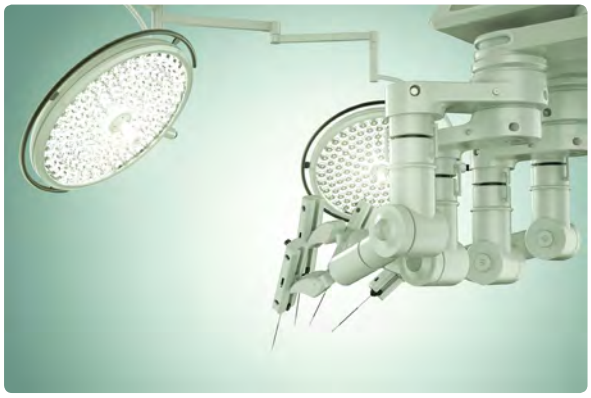
Innovations Driving Virtual Healthcare

In order for this approach to be viable, every facet of the healthcare ecosystem must adapt. Here are some of the technological innovations that are driving optimized, virtual healthcare.

Emerging Technologies

ROBOTICS

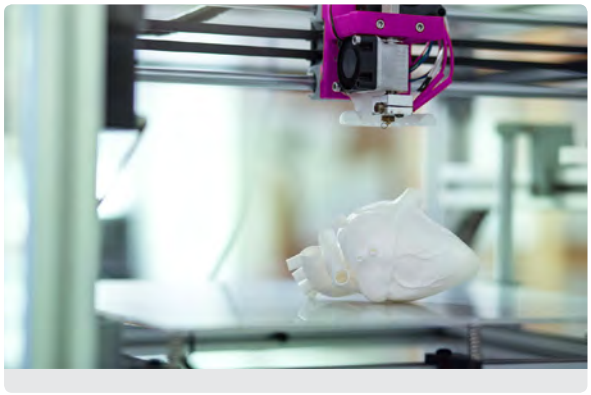
Robotics has been playing a growing role in a manufacturer's ability to produce goods more cost-effectively while eliminating and/or reducing product rejects. In healthcare, Intuitive's daVinci® surgical robot has allowed surgeons to perform complex procedures with improved precision, flexibility and control. The "brain" of the surgical robot lies within the vision cart and acts as a central computer to the operation of the robot itself. Robotic surgical systems have been shown to reduce surgeon fatigue while also reducing post-operative pain, thus improving the overall patient experience.



3D PRINTING

Many large global manufacturers have been employing the use of 3D printing for some time. The printer's ability to reproduce physical, working replicas of an organ, tool or part has resulted in significant advances in a patient's longevity while reducing waste and cost for providers.

The healthcare industry is harnessing the power of 3D printing to bioprint custom-made prosthetics, allowing surgeons to perform at a faster pace while reducing a patient's time in the OR.



POWER

Innovations like those mentioned above require a significant amount of power in order to calculate large amounts of data in real-time. As we have seen in recent advancements of the driverless and/or electric car, batteries that once powered a vehicle for 30 miles can now provide enough energy for 300 miles. This same technology is now being used in healthcare, enabling and extending advanced technologies utilized between doctor and patient.

Emerging Technologies, (cont.)

ARTIFICIAL INTELLIGENCE

Almost 25% of US homes have a smart speaker like Amazon's Echo which uses cloud-based intelligence to interact with your voice. Google and Microsoft are also in the space, and no doubt other consumer brands will soon follow. In healthcare, the use of AI may restore a person's ability to move or communicate after they have been affected by a disease such as ALS, or alert a nurse that sepsis is about to take hold of a patient even before they are symptomatic.

GENE EDITING

Expanding our understanding of DNA and the growth of CRISPR (Clustered Regularly Interspaced Short Palindromic Repeats) is making an enormous impact. In a world with people in need, CRISPR may be one of a long number of potential solutions to reduce or even end world hunger by significantly increasing the yield of a plant. This same kind of gene editing may be used to eliminate cancer cells or other infectious diseases.

Each of these five forces have the ability to significantly improve patient outcomes at a lower cost and validate that virtual medicine is coming of age.

Internet of Medical Things (IoMT)

The IoMT interconnects devices through data exchanges, enabling machine-to-machine interaction and real-time data streaming. When equipped with sensors, IoMT devices can vary from prostheses and implantable medical devices to medical equipment (e.g., stretchers) and home-use medical devices (e.g., blood pressure cuffs). Besides technology developments, there are other factors facilitating the growth of the IoMT including an aging population prone to various chronic diseases. Due to growing demand, experts predict that there will be between 20 and 30 billion devices within the IoMT by 2020.

There are three types of medical devices in use today that are ready to align with the shift to collaborative HDO / virtual patient care:

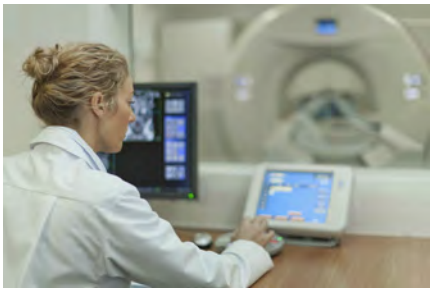
Medical Devices Currently Aligned to Collaborative HDO / Virtual Patient Care

Wearable External Devices

These devices incorporate biosensors to monitor patient data via remote/wireless communication which can be used for telemedicine and patient monitoring of blood pressure, EKG, temperature, glucose levels, oxygen levels, etc.

Implantable Medical Devices (IMDs)

These devices may replace a missing biological structure, support a damaged biological structure, or enhance an existing biological structure. This category includes implantable infusion pumps and other drug-delivery devices, cardiac pacemakers, implantable neuro-stimulator systems and glucose monitors.



Stationary Medical Devices

There is a wide range of stationary medical equipment, used for various applications like clinical operations (surgical devices) and connected imaging (x-ray and MRI machines), lab tests, patient monitoring, drug delivery, medication management, etc.

Innovating While Building Trust

The demand for trust in these technologies means that security considerations and measures must be considered at the forefront of development, as well as roll-out. Given the growth of connected medical devices, the potential for security lapses from release through use is considerable. While implanted devices draw the most attention, the broader universe of medical care gadgets can also warrant concern. In the US alone, hospitals can average anywhere between 10 to 15 connected devices per-bed. With this kind of scale, the number of security gaps can be significant.

Medical devices that feature wireless connectivity, remote monitoring, and near-field communication technology allow health professionals to adjust and fine tune implanted devices virtually and in real-time. Devices capture and transmit data across many channels and receiving parties. But many fail to incorporate data security protocols and standards. Older devices that remain in the field may be using outdated security software. There is also significant ambiguity on who owns the data – which can result in nobody taking the lead on managing current security practices.

Put all of these factors together and it's easy to understand why healthcare data is highly susceptible to security failures. Cyberattacks can be initiated by external bad actors, internal staff who make mistakes or a lax digital security implementation. Guidelines from the FDA are not mandated, and with a lack of funding and resources, comprehensive security efforts may be overlooked to achieve other organizational priorities.

In the US alone, hospitals can average anywhere between 10 to 15 connected devices per-bed. With this kind of scale, the number of security gaps can be significant.

Securing the New Perioperative Loop

So how can HDOs, EHRs and OEMs begin to tackle these challenges? By understanding that these rapid innovations that hold so much promise must drive us to think differently – bigger, really – and address the various moving parts at once. We've heard the adage of building and flying the plane at the same time. For all the benefits this new revolution is promising, those within the perioperative cycle must be confident that every input, every action and every device that's incorporated into the patient health plan is digitally secure.

IT'S ALL ABOUT THE DATA

There's a treasure trove of information captured and stored in healthcare and the prize money from insurance fraud and black market pharmaceutical sales can be extremely lucrative. Healthcare has the highest breach-related costs of any industry at $408 per-stolen record. As patients willingly share personally identifiable information (PII), often over open networks, reliable controls must be in place to protect patient privacy.

Think of your organization as an entity with identities. These identities are made up of people, applications and devices. Every identity has a role to play in the exchange of data. To create a secure environment for these data exchanges, every identity within the organization must be covered by layers of digital security.

Knowing where you are and where you want to go can be overwhelming. But breaking the process down into smaller bites can help ensure you're setting the stage for optimized data and device security without taking everything on all at once. Here are a few ways to get started:

01

IMPROVE THE STRENGTH OF TARGETED DEVICES

Establish the necessary barriers between the device and an outside threat. Understand what materials have gone into the construction of the device. Are these materials permeable? Easy to manipulate? Utilize features such as an auto-lock when the device leaves a certain area or space.

02

CONTROL ACCESS

Make sure you have a regular cadence in which passwords must be updated. Utilize multi-factor authentication when possible. How do you want to define your security protocol? Does the device being utilized have the ability to be patched?

Healthcare has the highest breach-related costs of any industry at $408 per-stolen record.

03

ON-SITE SECURITY

Ensure that when not in use, all devices are locked in a restricted, secure area. Be aware of your inventory at all times. No device should ever be left unattended.

04

ENCRYPT AND ENCODE

Authentication, authorization and encryption are the lifeblood of successful digital identity security. Unique digital certificates that cover every identity validate that a device is authentic and assert with high assurance that its messages are genuine. Encryption is Digital Security 101 to keep bad guys out of good data.

05

KNOW YOUR PARTNERS AND SUPPLIERS

Work with vendors and/or OEMs that have been vetted. Have an open dialogue regarding your vendor's attention to security. Seek to find common ground to know they place as much importance on security as you do.

06

INVEST IN DIGITAL SECURITY AUTOMATION

Manual processes are prone to errors. Automation drives high-assurance that every investment you've made in building your digital security program will work. Workflows become refined and execution gets easier.

07

PAY ATTENTION TO INDUSTRY GUIDELINES AND TRENDS

By following recommended standards, you should be reducing risk both inside and outside your organization. Regular cadences and audits on log files, pending digital certificate expirations, personnel changes and regulatory updates help detect issues and can provide the runway you need to prevent catastrophe.

08

BUILD A FLEXIBLE, COLLABORATIVE TEAM

The largest user groups of IoMT devices are doctors, nurses and biotechs. Provide opportunities to have two-way dialogue and input regarding security. Create shared responsibility in protecting patients.

Conclusion

KEYFACTOR SOLUTION

No matter how you're delivering healthcare today, security must be top of mind for both current processes and future innovations. Don't let the enormity of the mission result in in-action. Identifying the right partner can help you determine how best to invest in the right technologies.

Vendors like Keyfactor have a broad portfolio of enterprise and IoT security solutions specifically designed for the healthcare segment. With a proven platform and expanding capabilities designed for HDOs, EHRs, and OEMs, Keyfactor is helping transform and secure digital healthcare.

Vendors like Keyfactor have a broad portfolio of enterprise and IoT security solutions specifically designed for the healthcare segment.

ABOUT KEYFACTOR

Keyfactor™, formerly Certified Security Solutions (CSS), is a leading provider of secure digital identity management solutions that enables organizations to confirm authenticity, and ensure the right things are interacting in the right ways in our connected world.

From an enterprise managing millions of devices and applications that affect people's lives every day, to a manufacturer aiming to ensure its product will function safely throughout its lifecycle, Keyfactor empowers global enterprises with the freedom to master every digital identity. Our clients are the most innovative brands in the industries where trust and reliability matter most.

CONTACT US

- Visit: www.keyfactor.com
- Client Assistance: success@keyfactor.com
- 216.785.2990