Managing the Risk for Medical Devices Connected to the Cloud

cloud security alliance®

Acknowledgments

Lead Authors:

Dr. James Angle

Contributors:

Vincent Campitelli
Michael Roza

CSA Global Staff:

Shamun Mahmud

The CSA's Health Information Management Working Group aims to provide a direct influence on how health information service providers deliver secure cloud solutions (services, transport, applications, and storage) to their clients, and foster cloud awareness within all aspects of healthcare and related industries. The working group research was and will continue to be freely available for use without license fees or restrictions by the CSA.

Table of Contents

Introduction 5
Medical Device Security Life Cycle 7
- Pre-Purchase 7
- Post Purchase/Pre-Deployment 9
  - Network 9
  - Web Application Interface 10
  - Wireless Communications 10
  - Secure Communication Channels 11
- Deployment/Operations Management 11
  - Devices with Zero Degrees of Separation 11
  - Devices with One Degree of Separation 13
  - Devices with Two Degrees of Separation 13
  - Devices with Three Degrees of Separation 14
  - Devices with Four Degrees of Separation 14
- Decommission/Disposal 14

Recommendations and Conclusion 15
- Recommendations 15
- Conclusion/Need for Further Studies 16

References 18

Introduction

With the increased number of the Internet of Things (IoT) devices, Healthcare Delivery Organizations (HDO) are experiencing a digital transformation bigger than anything in the past. In addition to the regular IoT devices such as smartphones, HDOs also have IoT medical devices. The new breed of connected medical devices brings the promise of improved patient care, better clinical data, improved efficiency, and reduced costs; however, they also bring increased security risks (Armis, 2019). Many of these devices run on Commercial Off the Shelf (COTS) software such as Linux, Windows, and Oracle (Integrating the Healthcare Enterprise, 2009). Running COTS software makes the device susceptible to the same vulnerabilities as any other computer. Compounding the problem associated with COTS software, device manufacturers continue to use old technologies such as Windows CE 6 or embedded older versions of Linux or other outdated Windows. This is due to the time required to gain approval for medical devices. This means device manufacturers sell devices when the software has already passed the main software support period when patches and updates are no longer available.

Today's medical devices can and often do connect to the cloud, which increases the risk of using outdated software by increasing the attack surface. An example of these are implanted medical devices that connect through a transmitter to the HDO. This process may include the use of the cloud. This presents the HDO with threats and vulnerabilities that include technology issues, software risks, and human factors.

This paper categorizes the risk management functions into multiple areas. The assumption made is that the organization has identified the threats found in the risk analysis. This premise is based on the requirement for the HDO to conduct a risk analysis, which should include the identification of threats, vulnerabilities, likelihood of attack, and impact. The first area describes requirements for purchasing new devices to ensure the identification and mitigation of vulnerabilities prior to implementation. Next is The second section describes how to manage the risk using degrees of separation from the patient, since how devices are managed is directly related to the proximity of the device to the patient. An implanted device cannot be managed the same way as can an ultrasound machine. As part of the evaluation, the controls should be evaluated using the Cloud Security Alliance (CSA) Internet of Things (IoT) control framework. The CSA IoT Security Controls framework allows an organization to evaluate and implement an IoT system within their ecosystem. The control framework produced by the CSA IoT working group is being expanded by the CSA Health Information Management working group to include the Medical IoT (MIoT) to focus specifically on medical devices. The MIoT Security Control Framework is relevant for HDOs that incorporate multiple types of connected devices, cloud services, and networking technologies (Cloud Security Alliance, 2019).The final area deals with continuous monitoring of the devices to ensure the mitigating control effectiveness. Table 1 displays the degrees of separation and other relevant information.

Degrees of Separation	Definition	Device Support Responsibility
0 degrees	The device is implanted in the patient.	Vendor and/or Physician or Medical Staff
1 degree	The device touches the patient.	Vendor or Clinical Engineering
2 degrees	The device does not touch the patient, but it is taking measurements of patient vital signs, fluids, or data.	Vendor or Clinical Engineering
3 degrees	The device does not touch the patient, but it may be doing something still vital to proper patient diagnosis.	Vendor or Clinical Engineering
4 degrees	The device is removed from the patient and is an operational tool more than a diagnostic or clinical device.	Vendor or IT

Table 1 degrees of separation from the patient

Goal

The goal of this paper is to present the concept of managing the risk of medical devices connected to the cloud based on their proximity to the patient and introduce practices to secure the use of cloud computing for medical devices. The degrees of separation are based on how the device interacts with the patient, that is, whether the device is implanted or completely separated as it is with 4 degrees of separation.

Target Audience

The target audience for this document are people in cybersecurity, enterprise architecture, clinical engineering and compliance roles within the healthcare industry. These stakeholders will be largely responsible for the evaluation, deployment, and management of medical devices within their enterprise.

Secondarily, solution providers, service providers, and medical device vendors will also benefit from reading this document.

Medical Device Security Life Cycle

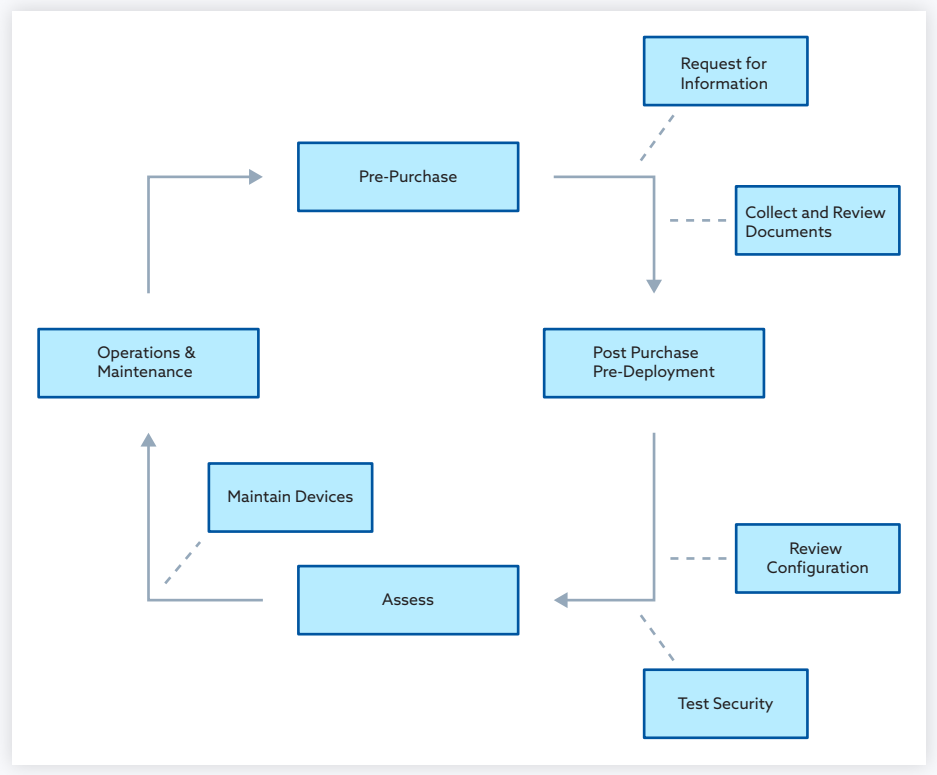

Figure 1 Medical Device Lifecycle

Purchasing (Pre-purchase to Post-purchase/Pre-deployment)

Pre-purchase

Many HDO medical device-purchasing decisions are made without the input of all stakeholders, which is not ideal considering that decisions should be risk-based and allocated among the relevant personnel in all affected departments (Hinrichs, Dickerson, and Clarkson, 2013). An HDO should take specific steps before purchasing new medical devices. Purchasing new medical devices should be a multifunctional effort with representation from clinicians, clinical engineering, IT, and information security (Graves, 2011). The information security representative should assess the requirements for running, supporting, and securing the device (O'Brien, 2014). The FDA defines cybersecurity as "the process of preventing unauthorized access, modification, misuse, or denial of use, or unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient" (Center for Devices and Radiological Health, 2014 p. 3). To this end, the FDA recommends that manufacturers follow the cybersecurity framework established by the National Institute of Standards and Technology (NIST). The NIST cybersecurity framework 1.1 requires manufacturers to address the following core functions: Identify, Protect, Detect, Respond, and Recover (National Institute of Standards and Technology, 2014).

The HDO is required by HIPAA rule 164.308(a)(1)(ii)(A) to perform a risk analysis on the device. The FDA recommends the HDO maintain the following documentation on the cybersecurity of devices:

> 1. Hazard analysis, mitigations, and design considerations pertaining to the cybersecurity risk associated with their device;
> 2. A traceability matrix linking the cybersecurity controls to the risk considered;
> 3. A plan for providing validated updates and patches throughout the device lifecycle;
> 4. A summary of security controls in place ensuring the integrity of the software; and
> 5. Instructions including specifications related to the cybersecurity controls.

It should be kept in mind that these are only recommendations and are not required by the FDA (Center for Devices and Radiological Health, 2014).

A good starting point is requiring the manufacturer to provide the Manufacturer Disclosure Statement for Medical Device Security (MDS2). The form is the result of collaboration between the Health Information Management System Society (HIMSS) and the National Electronic Manufacturers Association (NEMA). The MDS2 contains the device description, information on the management of private data, and information on the security capabilities of the device (NEMA, 2013). While no regulatory requirement exists for the manufacturer to fill out the MDS2 form, the recommendation is for the organization to require the form.

These documents provide the HDOs with the information necessary to make a risk-based decision on the purchase of the device. Having the information to make a risk-based decision prevents a situation where the HDO purchases a device and then discovers the device has little or no built-in security controls. If an HDO purchases a device without reviewing the security controls, the decision to use the device is based upon the economics and other features but ignores the security risk.

After making the purchase decision and prior to the actual purchase of the device, personnel involved must include security requirements in the contract. The contract should require the manufacturer to supply a life-cycle management plan for the device, including how the manufacturer will manage the operating system software when the support for the software is discontinued as well as which party is responsible for patching and software updates. When the responsibility for installing the patches lies with the manufacturer, a time requirement for completion should be included. When the HDO is responsible for installing the patches, a time requirement for the manufacturer to supply the patches should be included. Table 2 gives an example of time requirements for supplying patches based on the criticality of the vulnerability.

Criticality	Time Requirement
Critical	1 week
High	2 week
Moderate	3 week
Low	4 week

Table 2 Timing of patch cycles versus criticality of vulnerability

The determination of the time requirement depends on organizational risk tolerance and the manufacturer's ability to test and deliver the patches. In addition to the above requirements, HDOs must insist that manufacturers follow secure coding practices throughout the device lifecycle.

Post-Purchase/Pre-Deployment

Once a medical device is purchased, testing of the device is required before it can be connected to the HDO's network and the cloud. A good approach is for the security engineer to follow these steps:

1. a configuration review, examining the configuration information collected during the pre-purchase assessment. The documents should include a listing of all interconnections and a data flow diagram;
2. a Nmap scan to identify all open ports and protocols used. Nmap is an open source network exploration and auditing tool;
3. a vulnerability scan using a product like Nessus or Qualys;
4. a configuration scan; and
5. penetration testing: Taking advantage of discovered vulnerabilities, security engineer should perform further exploitation such as installing? malware, searches and downloading data from the compromised device, or attempts to disable functionality.

Conducting these tests will allow the HDO to understand the security posture of the device as well as to identify vulnerabilities that require mitigation. The HDO can also conduct more specific testing based on what they find and how the device connects to the network and the cloud. The following are some examples of additional testing that can be done:

NETWORK

- Recon
  - Review of manual
  - Review of technical specifications
  - Review of configuration

- Discovery
  - Identification of network ports
  - NMAP
  - Test for UID/passwords
  - Manual / scripted
  - Brute-force well-known passwords
  - Hydra - password brute-forcing
- Vulnerability Scanning
  - Identification of vulnerabilities
  - Nessus / Qualys
  - Validation of findings
  - Protocol specific testing: telnet, ssh, ftp, snmp, http, ssl (TLS) weaknesses
  - Authorization traverse (non-admin > admin user)

WEB APPLICATION INTERFACE

- Recon
  - Review of manual
  - Review of technical Specifications
  - Review of configuration
- Discovery
  - Identification of web application ports(from NMAP above)
  - Running Nikto discovery
  - Spidering the website
  - Web directory brute force
  - Test authentication method
  - default UID/passwords
  - brute-force well-known passwords
  - Hydra- password brute-forcing
- Vulnerability Scanning
  - Running Web Inspect / Burp Suite scan
  - Testing for specific code-injection vulnerabilities
  - Testing direct-page access –Bypass
  - Authorization traverse (non-admin > admin user)

WIRELESS COMMUNICATIONS

- Recon
  - Review of manual
  - Review of technical specifications
  - Review of configuration
- Discovery
  - Scanning for device's broadcasting for access points
- Vulnerability Scanning
  - Ensuring that device is not attaching to unknown access points
  - Testing other wireless communication methods

- ZigBee
- Bluetooth

SECURE COMMUNICATION CHANNELS

- Secure communication testing
- sniffing traffic to ensure the security and confidentiality of traffic
- looking for broadcasts
- looking for outbound, unsolicited traffic (vendor, cloud, third party)
- communication with other internal devices, server databases

In addition to finding vulnerabilities, testing will show the resilience of the device. Afterwards, the HDO? will know which devices can be scanned while in use as well as those that cannot be scanned.

Deployment/Operations Management

Operations management of medical devices is a complex and time-consuming process with multiple working parts. How the devices are managed, controlled, and updated depends on the device and its proximity to the patient. Implanted devices are not managed the same way as an imaging device. The following sections explain how the different devices can be managed based on their proximity to the patient.

DEVICES WITH ZERO DEGREES OF SEPARATION

Implanted Medical Devices (IMD) present a unique set of issues due to the multitude of parts requiring continuous monitoring for vulnerabilities. Connecting an IMD to the Internet/cloud requires at least three, and in some cases four, different devices.

The first is a device that is implanted in the patient. This can be any one of several different types of device; however, regardless of the type of device, they all have common features. The device does not on its own connect directly to the Internet/cloud. In older devices the connection is to an intermediary device using Radio Frequency (RF). In newer devices the connection to the intermediary device is most often made using Bluetooth.

The second device is the intermediary device which connects to a base station that connects either wired or wirelessly to the Internet/cloud. An alternative means of connecting is for the intermediary device to connect to a smart device (phone or tablet) and then to the Internet/cloud.

The final step is the connection to the Internet/cloud. Every step along the way presents a security challenge that must be addressed. There will always be patches and upgrades that will need to be applied to each device. To complicate the process, if a smart device is used, it will likely be completely controlled by the patient.

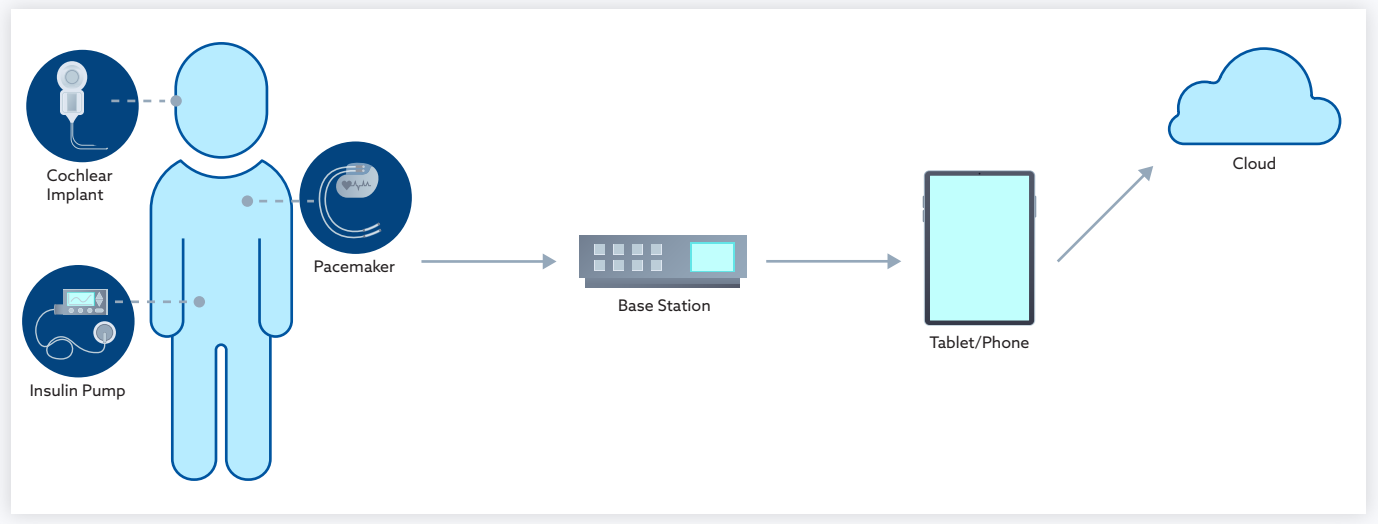

Figure 2 Implanted device connection

Assuming the HDO completed all the testing outlined above and remediated all vulnerabilities, there are two issues left to address:

1. How does each device accomplish Identity and Access Management (IAM)?
2. How does the HDO ensure that additional vulnerabilities discovered are remediated?

Both issues are by no means easy to resolve. These current IAM issues are a risk at the device level and not easily mitigated. Currently devices connect to the Bluetooth simply using the device embedded code. Hence, there is no effective authentication control.

IAM remains an issue whether the intermediary device connects to the Internet/cloud or to a smart device.

The need for security and protection of privacy is essential, and adding secure authentication enhances both security and privacy. Introducing secure authentication strategies or secure database access after development is common but risky. The manufacturer can avoid this mistake by considering and designing for security in the early stages of development. The manufacturer should include a selectable password or pin for connecting to their devices. While a pin or weak password is not ideal, it would provide a measure of security not currently present in the devices.

Personal devices using a manufacturer's smart device apps should be programmed to use multifactor authentication. This is not difficult to program and helps ensure the protection of the user's data. Additionally, if the device allows for the use of a personal device, either the manufacturer or the HDO should at a minimum provide the patient with some information about securing their personal device and emphasizing the need for security.

Remediation of newly discovered vulnerabilities presents the manufacturer with the challenge of effective and timely patching. Can they simply push a patch? Does patching require the patient to visit the HDO in order to patch the device? The answer depends on the function of the device. There are some, such as a pacemaker, that should not have patches pushed without involving the HDO.

Regardless of how the device is patched, both the manufacturer and the HDO must have a plan in place to ensure the device continues to function as designed. The plan should include how to communicate this to the patient as well as how the patching process will proceed. Additionally, the plan should include a timeline for applying patches and upgrades that ensures a timely completion that protects the safety of the patient.

DEVICES WITH ONE DEGREE OF SEPARATION

Figure 3 Infusion Pump

Medical devices that touch the patient include those like infusion pumps that administer medications. These devices are often connected to the network and in some cases the Internet/cloud. The devices can send data directly to the patient's Electronic Health Record (EHR). These devices are connected either without authentication or weak authentication. The devices use a common Operating System (OS) such as Windows or Linux. The OS can also be an embedded version. Unfortunately, all of the operating systems options can contain vulnerabilities.

As with implanted devices the two biggest issues are IAM and patching/updating the system. When the device uses one of the standard OSs it should have strong authentication added to the device. Because these devices are connected to the patient, they cannot be patched or updated while they are in use.

These devices are most often connected to the HDO network and then if the cloud is used, they are routed to the cloud. For ease of use many of these devices do not have any IAM. The absence of this security feature exposes the manufacturer's device to unauthorized and undetected access. In order to protect the device manufacturers, they need to include IAM to their products.

Since updating and patching the device cannot be done while it is connected to the patient, the HDO should isolate the device on a segmented network and apply compensating controls to the network to protect the devices until they can be patched. Many devices cannot have antivirus or other endpoint protection added to them, so HDOs must control the flow of data going through the segmented network. All medical devices of this type require scheduled maintenance. Updating and patching should be a part of the scheduled maintenance.

While Using the maintenance windows to ensure updating and patching is completed, it will not keep the devices completely up to date, which is why network segmentation and compensating controls are essential.

DEVICES WITH TWO DEGREES OF SEPARATION

Devices with two degrees of separation do not touch the patient, but they are doing measurements with of patient vital signs, fluids, or data. While these devices are not directly connected to the patient, it is imperative that the integrity of the data be protected. When a medical device gives inaccurate information, it can result in both incorrect diagnosis and treatment.

Figure 4 Vital Sign Monitor

The issue is the lack of IAM. These devices can connect to the HDO's network and send data to the Internet/cloud. The lack of authentication makes both the device and the cloud vulnerable. At the very least, they should have basic access control such as a pin.

Since these devices are not directly connected to the patient they can be patched and updated as these become available from the vendor. The vendor must approve all patches and updates to ensure they do not change the functionality of the device.

DEVICES WITH THREE DEGREES OF SEPARATION

Devices with three degrees of separation do not touch the patient, but such a device may be doing something vital to proper patient diagnosis. An example is radiology equipment or laboratory equipment. Although these devices are not connected to the patient, their functionality and integrity are vital to the diagnosis, treatment, and safety of patients.

Some of the devices, particularly radiology devices, have good IAM capabilities; however, in this researcher's experience the login is often bypassed for convenience. Often laboratory equipment lacks good IAM capabilities, which presents an issue when data is stored in the cloud.

Figure 5 Image Viewer

As with the devices with two degrees of separation, these devices can be patched and updated as soon as the vendor approves the patches and updates.

DEVICES WITH FOUR DEGREES OF SEPARATION

Devices with four degrees of separation are removed from the patient and are an operational tool more than a diagnostic or clinical device. An example is equipment used to monitor the patient's environment such as bed monitors and room monitors. While these devices are not used for patient care, they are critical for patient safety.

These devices do not have any IAM capabilities, and they can be patched as soon as patches are available.

Decommission/Disposal

While the decommission/Disposal of medical devices is not pertinent to this paper, it warrants further review and will therefore be researched and elaborated in a future publication.

Recommendations and Conclusion

Recommendations

Clearly, connected devices present a risk that could endanger the wellbeing and even the lives of our patients. After conducting a risk assessment and security review, the next thing the HDO should do is to enhance the device's capability regarding authentication. One of the primary methods for security outlined in the FDA's Content of Premarket Submissions for Management of Cybersecurity in Medical Devices is to prohibit untrusted users from gaining access to these devices by enabling strong authentication.

The ability to secure data and limit who has permissions to view and use the data is not a new idea. The question is why medical devices were not subject to authentication rules to start with. Since many medical devices do not have the capability for username and passwords or since including these would be impractical, a solution would be to use PKI (public key infrastructure) where digital certificates prove the authenticity of the device.

Digital certificates would ensure a level of trust in the medical device that may otherwise be lacking and, when combined with applications to monitor the infrastructure, could identify and prevent access to uncertified devices.

Medical devices that connect to the Internet/cloud through the user's smart device should require Multi Factor Authentication (MFA). In today's Internet/cloud environment, sites, including government as well as business, often require MFA. MFA is prevalent on these sites to protect the user's data; isn't medical data as important?

Some medical devices do not have the ability to authenticate; in these cases the use of an authentication gateway should be the standard practice. A gateway can perform several functions. In addition to authentication, it can be used for translating protocols, encrypting, processing, managing and filtering data. In the medical device ecosystem, a gateway sits between devices and sensors to communicate with the cloud.

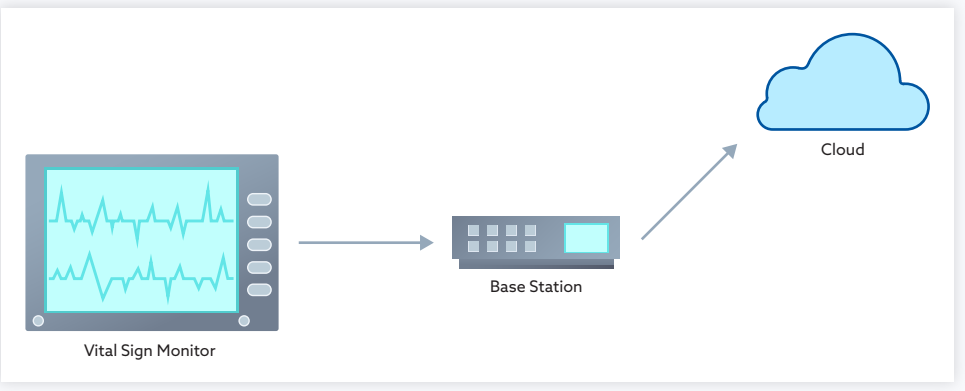

Figure 6 Authentication Gateway

Continuous monitoring will help ensure that both the HDO and the cloud provider maintain the desired security posture. One essential tool is a cloud access security broker. According to Gartner,

> "Cloud Access Security Brokers (CASB) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on" (Gartner, 2019).

The CASB will ensure the HDO knows what devices are connecting to the cloud, what data is being sent to the cloud, and what cloud provider the data is sent to.

The HDO must also ensure that all regulatory requirements are fully satisfied. If the device is sending PHI, then a business associate agreement is required. If there is any question about this requirement, the OCR website should be consulted for clarification.

The HDO should also monitor the Cloud Security Alliance top threats list, which is an annual list of the top cloud threats. The document includes the business impact for each threat, the key take-away, CSA security guidance, and the controls used to help mitigate the threats. Mitigating the top threats will go a long way towards securing the medical device connections as well as the cloud provider. When dealing with implanted medical devices, it is imperative that the HDO educate the patient about the threats associated with sending their data to the cloud. Poor security practices put the patient, as well as the cloud provider, at risk. This in turn could put other patients at risk.

It is imperative to ensure the HDO has good policies and procedures in place and that they are followed.

Conclusion/Need for Further Studies

The number of files with sensitive data shared in the cloud has increased fifty-three percent year over year. The use of cloud computing in healthcare will continue to increase in the future. As the number of files stored in the cloud has increased, the percentage of files that contain sensitive data has also grown. Today twenty-one percent of files stored in the cloud contain sensitive data, of which nine percent contains PHI (McAfee, 2019).

Healthcare cloud services can provide applications to HDOs that otherwise would not be available. Additionally, the increased use of the medical devices connected to the cloud will accelerate as cloud use increases. Healthcare-related cloud services are complex and cover almost all aspects of healthcare delivery. While security of healthcare information is a major concern for HDOs and cloud computing is not without risk, there have been significant efforts by organizations like the Cloud Security Alliance to ensure these risks are addressed and mitigated. By following the guidance provided and doing due diligence, HDOs can minimize the risks and maximize the benefits of cloud computing.

According to the CSA

Top Threats in Cloud Computing" report suggests an interesting and somewhat new perspective on cloud security. This new outlook focuses on configuration and authentication and shifts away from the traditional focus on information security (e.g., vulnerabilities and malware). Regardless, these security issues are a call to action for developing and enhancing cloud security awareness, configuration and identity management." (CSA, 2019 p.40)

While research on medical devices connected to the cloud has advanced significantly, additional research is required. Of interest is research into the use of Blockchain as a means of securing medical devices and their associated data connected to the cloud. Currently there are several on-going efforts such as the Cybersecurity subgroup, IEEE which is working on developing a new cybersecurity framework for the use of Blockchain in highly regulated industries of healthcare and life science and the CSA work group Cybersecurity Best Practices for Blockchain Technology Use in Healthcare—A Risk Management Framework.

In addition, there are working groups devoted to the issues of IoT devices. The CSA IoT work group has produced the IoT control framework and is working with the Health Information Management working group to expand the control framework to include medical devices. The IoT Controls Framework allows organizations to tailor security requirements to their specific IoT system implementation. Common components within an IoT system--including At the Edge, In the Network, and In the Cloud--have been identified with corresponding requirements (CSA, 2019).

References

Armis (2019), Medical and IoT Device Security for Healthcare, Retrieved from https://www.armis.com/resources/iot-security-white-papers/medical-iot-device-security-for-healthcare/

Center for Devices and Radiological Health, (2014). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Retrieved from https://www.fda.gov/regulatory-information/search-fda-guidance-documents

Cloud Security Alliance (2019) The Egregious 11 - Top Threats to Cloud Computing + Industry Insights, Retrieved from https://cloudsecurityalliance.org/group/top-threats/

Cloud Security Alliance (2019) Guide to the CSA IoT Security Controls Framework, retrieved from https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework/

Dempsey, K., Chawla, N. S., Johnson, A., Johnson R., Jones, A. C., Orebaugh, A., Scholl, M., & Stine, K. (2011). Information Security Continuous Monitoring for Federal Information Systems and Organizations (Special Publication No. 800-137). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/ FDA, October 2014, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

Gartner, November 2019, Cloud Access Security Broker, Retrieved from https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs

Graves, K. (2011). Global Best Practices in Medical Device Procurement – A road Map to System Success. Journal of Medical Marketing, 11(2), 101-108. doi: 10.1057/jmm.2011.1

Hanna, S., Rolles, R., Molina-Markham, A., Poosankam, P., Fu, K., & Song, D. (2011) Take Two software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices. Paper presented at the 2nd USENIX workshop on health security and privacy, San Francisco, CA. Abstract retrieved from https://spqr.eecs.umich.edu/papers/hanna-aed-healthsec11.pdf

Healey, J., Pollard, N., & Woods, B. (2015). The healthcare Internet of Things: Rewards and risks. Retrieved from the Atlantic Council website: https://www.atlanticcouncil.org/wp-content/uploads/2015/03/ACUS_Intel_MedicalDevices.pdf

Hinrichs, S., Dickerson, T., & Clarkson, J. (2013). Stakeholder Challenges in Purchasing Medical Devices for Patient Safety. Journal of Patient Safety 9(1), 36-43. doi: 10.1097/PTS.0b013e3182773306.
McAfee (2019), Cloud Adoption and Risk Report, Retrieved from https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-adoption-risk.html

Mc Caffery, F., Burton, J., & Richardson, I. (2010). Risk Management Capability Model for the Development of Medical Device Software. Software Quality Journal 18, 81-107. doi: 10.1007/s11219-009-9086-7

National Electrical Manufacturers Association, (2013) HIMSS/NEMA Standard HN 1-2013, Medical disclosure statement for medical device security. Retrieved from www.himss.org/resourcelibrary/MDS2

National Institute of Standards and Technology, (2014). Frameworks for Improving Critical Infrastructure Cybersecurity. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

O'Brien, G. (2014). Wireless medical infusion pumps (Use case). Retrieved from The National Institute of Standards and Technology website: https://nccoe.nist.gov/sites/default/files/nccoe/NCCOE_HIT-Medical-Device-Use-Case.pdf