Pulse Secure®

Implementing HIPAA Security Rules – Challenges and Best Practices for IT in the Health Care Industry

Table of Contents

Introduction

All health care related organizations must adhere to the standards laid down by HIPAA (Health Insurance Portability and Accountability Act of 1996) to protect a patient's personal health information.

This document outlines key challenges faced by health care organizations today, and how to successfully overcome such challenges and ensure that networks, data and applications remain secure.

About Pulse Secure

Pulse Secure's mission is "Delivering Secure Access Solutions for people, devices, things and services". Remote Access to data center resources has evolved to Secure Access – where the location and type of resource being securely accessed is more than just data centers, including Cloud/SaaS applications, and Mobility. Devices must be secured whether outside or inside the organization, laptop or mobile.

Pulse Secure Access Suite is a comprehensive Secure Access solution that securely connects workers to company resources and protects company devices, regardless of location – in the data center, cloud or mobile. Pulse Secure delivers access to all company resources via a single client or mobile application – dramatically simplifying access and increasing user productivity.

Administrators configure contextual access policies to control access based on devices, locations, resources, users and groups, or even endpoint profiling. Policies can be extended to internal networks, allowing organizations to identify, profile, secure, and manage internal devices, Guest User access, and even BYOD devices. Detailed management and reporting meets the needs of the toughest regulatory compliance environments.

Pulse Secure is well positioned to deliver comprehensive Secure Access, given our 15+ years of experience, over 20,000 customers and 20 million endpoints.

Exponential Increase in the Number of Network Devices

With the rise of IoT (Internet of Things), many devices used in health care are now able to communicate over the Internet. From wifi-enabled pacemakers to blood pressure monitors, all of them can now be used to monitor the patient's health over the Internet. In fact, the number of medical devices with Internet-connectivity has increased so dramatically over the past few years, there is a new acronym to describe it - IoT-MD (IoT Medical Devices). And it's not just IoT-MD that's exploding - hundreds of electronic devices such as IV pumps, physiological monitors, X-Ray machines and MRI scanners used in hospitals are being connected to the network so that patient data can be collected, analyzed and stored. A recent report from HIMSS.org indicates there might be up to 10 to 15 medical devices per bed - resulting in over 7500 medical devices for a typical 500-bed hospital.

While connecting medical equipment to a network is incredibly useful, it also poses some serious security threats.

1. Medical devices are not usually updated with the latest security patches.
2. Often, an IoT-MD device may be connected to the network with the default management password set at the time of manufacture.
3. The inability to deploy agents (e.g. SNMP) to manage medical devices is another limitation.

If an attacker can exploit a vulnerability in one of these devices, he or she may be able to gain access to the network and steal patient data. Or worse.

To conduct a "thorough risk assessment" (Section 164.308 (a)(1) of the HIPAA standards), a health care organization must first **know the complete list of devices** that are connected to the network because you simply cannot protect what you cannot see. Once the list of devices is known, the risk assessment must be performed based on Operating System, type of device, device use, applications installed on the device, IP addresses, etc.

Policies must then be created to automatically place "suspicious" or "vulnerable" devices in a quarantine zone, while allowing compliant devices to connect to the network. Finally, the network must be monitored continuously to ensure no rogue devices gain access to sensitive data.

Pulse Profiler is able to scan networks and display all the devices on the network along with their characteristics such as operating system, IP address, type of device, port connections, last connected time, etc. Using a combination of periodic scans and real-time updates, Pulse Profiler can monitor the network constantly to ensure that the device inventory is kept up-to-date.

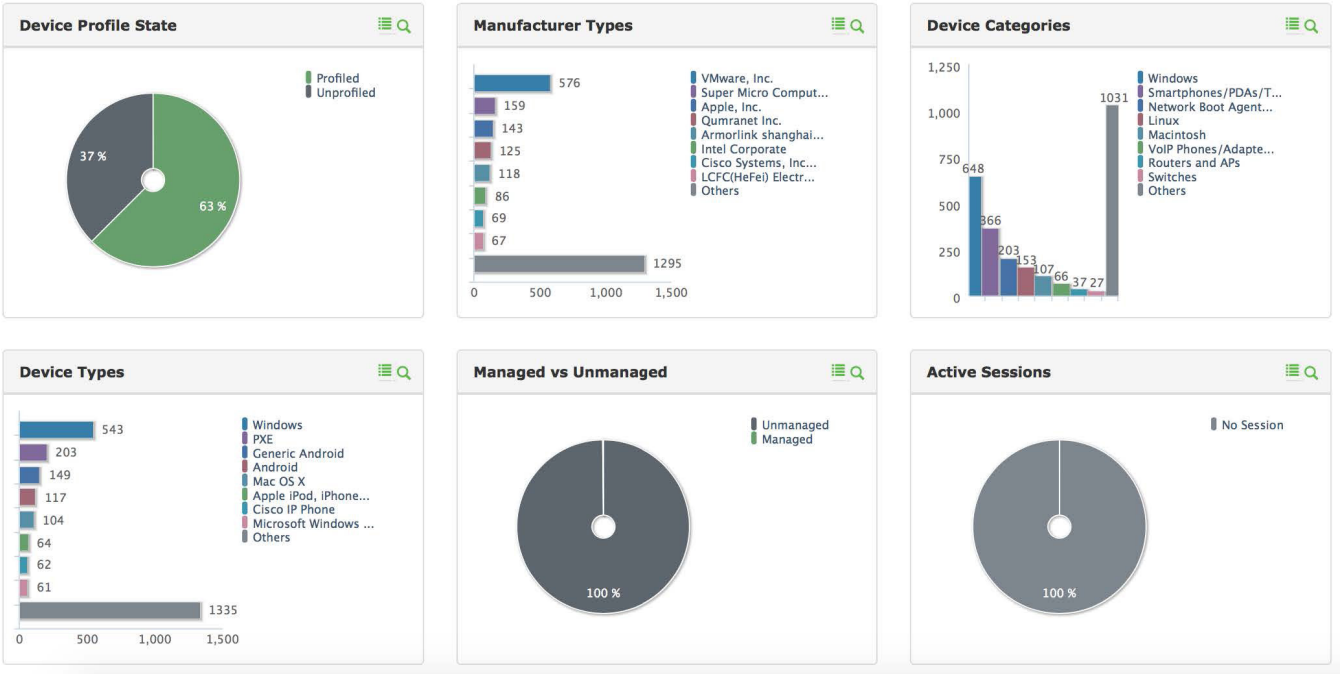


Figure 1: Profiler Dashboard

Using Pulse Policy Secure can mitigate risk to the corporate network by applying fine-grain device access policies to allow only the approved types of devices to access the network. For example, contractors can be prevented from attaching their devices to the network by creating a rule in Pulse Policy Secure that allows only corporate-owned devices on the network.

The Rise and Rise of BYOD

Health organizations are encouraging employees to use their own mobile devices to access electronic patient health information (or ePHI). A recent report from Manhattan Research suggests that "almost 45% of all physicians use smartphones to access digital resources for professional purposes between patient consults, and almost one in four during patient consults". The benefits are obvious - reduced costs in purchasing and maintaining inventory for the organization, and for the doctors it's the convenience of carrying just one device for both personal and professional work.

But just like IoT-MD, this trend is fraught with risk too - if the mobile device owned by the doctor is compromised, or stolen - it could result in loss of privacy of sensitive patient data. Apart from the financial penalties, this can lead to loss of reputation and have a significant impact on the future of the organization.

The OCR breach portal that maintains a list of breaches of unsecured protected health information reported that almost 80% of the breaches reported in 2016 were due to loss or theft of mobile devices. These devices contained patient data on an un-encrypted drive making it very easy to steal information off the device.

Other problems associated with mobile devices include installing applications that appear harmless, but are in-fact malicious in nature and can be used to hack into the device. Once these "Rooted" devices connect to the network they can propagate malware and capture sensitive data.

An effective way to mitigate these threats is to use a Mobile Device Management (MDM) solution to manage all the mobile devices. Mobile Devices can be configured with policies that ensure that only devices that comply with company policy can connect to the network - others are sent to a quarantine zone, where they will need to be remediated before admitting them back to the corporate network. Some of the capabilities of a MDM solution include, the ability to:

1. Retire lost, or stolen devices by remotely wiping all ePHI while leaving personal content untouched on the device.
2. Prevent users from installing apps that are not in a "pre-approved" list.
3. Perform periodic audits to ensure device is still compliant with corporate policy.

Pulse Workspace, which is available in the advanced edition of the Secure Access suite is a cloud-based MDM solution that is easy to setup and configure with all the capabilities listed above and a lot more.

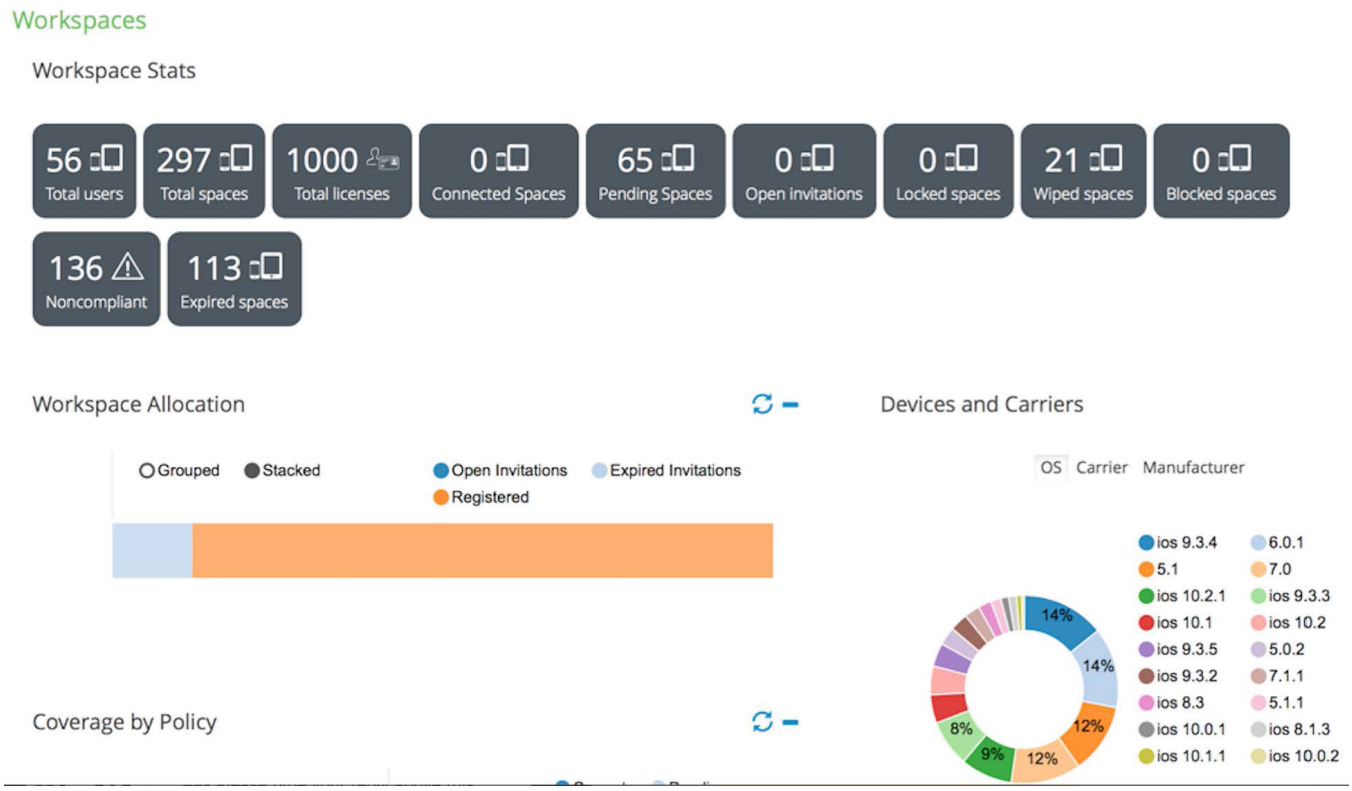


Figure 2: PWS Dashboard

Growing Ecosystem of Contractors, Partners, Clinicians…

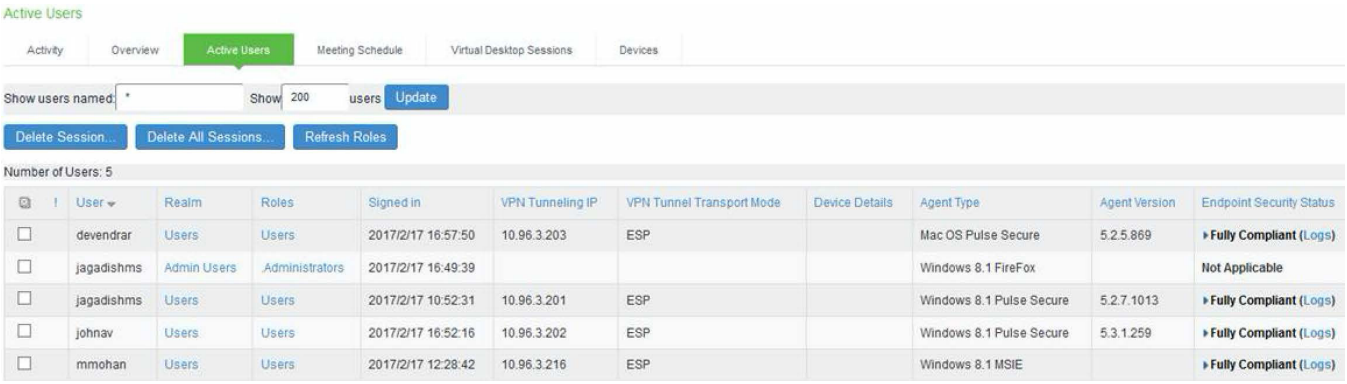
Today's networks are extremely complex with various types of users connecting to the same network to get their work done. While a doctor may connect to the network to access a patient's medical history, a person from the hospital staff may need to access the same network for conducting research-related tasks. Guests and patients may also connect to the network to simply access the Internet.

In all these cases, it is extremely important to ensure that proper authentication is performed, and that, once the user is logged in, only appropriate resources are made available to that user.

The "Technical Safeguards" section of HIPAA, under the HIPAA security rule (Section 164.312) deals with the implementation of authentication and authorization systems that health care organizations must put in place.

Implementing the specifications mentioned in the "Technical Safeguards" section requires the use of assigning a unique user ID for each person that has access to the network. Furthermore, roles may be assigned to the logged in users to restrict their rights to only have access to what is required of them to get their job done. Proper audit control mechanisms are also important in this regard - it should be possible for investigators to know all details about a breach including the user who accessed the data, the time of access, access location, etc.

Both Pulse Connect Secure and Pulse Policy Secure can be configured to authenticate users based off an identity store such as Microsoft's Active Directory or LDAP. These solutions also contain an extensive role-based access control framework that can be used to implement fine-grain access based on type of user. All user activities are available to the admin via the user access logs for reporting and analysis. Logs can also be configured to be sent to remote syslog servers so they may be stored for a greater period in a central location.



	User	Realm	Roles	Signed in	VPN Tunneling IP	VPN Tunnel Transport Mode	Device Details	Agent Type	Agent Version	Endpoint Security Status
☐	devendrar	Users	Users	2017/2/17 16:57:50	10.96.3.203	ESP		Mac OS Pulse Secure	5.2.5.869	Fully Compliant (Logs)
☐	jagadishms	Admin Users	Administrators	2017/2/17 16:49:39				Windows 8.1 FireFox		Not Applicable
☐	jagadishms	Users	Users	2017/2/17 10:52:31	10.96.3.201	ESP		Windows 8.1 Pulse Secure	5.2.7.1013	Fully Compliant (Logs)
☐	johnav	Users	Users	2017/2/17 16:52:16	10.96.3.202	ESP		Windows 8.1 Pulse Secure	5.3.1.259	Fully Compliant (Logs)
☐	mmohan	Users	Users	2017/2/17 12:28:42	10.96.3.216	ESP		Windows 8.1 MSIE		Fully Compliant (Logs)

Figure 3: List of active users

HIPAA Compliance and the Secure Access Suite

The table below summarizes the various steps you can take to fulfill some of the technical requirements relating to HIPAA's Technical and Administrative safeguards standards.

Table 1: 164.312 Technical Safeguards

Standards	Implementation Specifications	Configurations for Compliance
164.312 (a)(1) Access Control Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a).	**164.312(a)(2)(i)** Unique User Identification Assign a unique name and/or number for identifying and tracking user identity.	Integrate PCS and PPS with identity stores such as AD/LDAP that enforce unique user identifications. This makes all actions attributable to the specific individual. Set granular access to different types of employees using role-based access control framework in PCS/PPS so that they can only access "just" the information they need to do their job.
	164.312(a)(2)(iii) - Automatic Logoff Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Set sessions timeouts on PCS/PPS so that user is logged off automatically once a specified time interval has elapsed.
	164.312(a)(2)(iv) - Encryption and Decryption Implement a mechanism to encrypt and decrypt electronic protected health.	When allowing remote access to applications use PCS - this will ensure that all transfer of ePHI information is performed over an encrypted channel.
164.312 (b) - Audit Controls Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.		PCS and PPS automatically create log entries each time any device connects to your network. Both successful and unsuccessful connections are logged. This information can be reviewed periodically, at PCS/PPS, or centrally using P1 (if deployed).
164.312 (d) - Person or Entity Authentication Implement procedures to verify that a person or entity seeking access to electronic protected information is an authorized user.		Set authentication server in PCS/PPS to use AD/LDAP etc. Configure Profiler to only allow authorized devices to access ePHI information.
164.312 (e)(1) - Transmission Security Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	**164.312(e)(2)(ii)** - Encryption Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	All transmission of data between endpoints containing ePHI information and PCS is encrypted. Ensure that all mobile devices are encrypted using policy enforcement from PWS. Additional controls like remote-wipe option should also be configured in the PWS policy so that ePHI information can be wiped from the mobile devices in case they were lost or stolen.
164.310 (d)(1) - Device and Media Controls		With cloud apps becoming ubiquitous, many companies are moving away from portable media. Use Cloud Secure to securely access HIPAA compliant applications for file-sharing etc. As a bonus, you have audit control built in when using this option.

Table 2: 164.308 Administrative Safeguards

Standards	Implementation Specifications	Configurations for Compliance
164.308(a)(1) - Security Management Process Implement policies and procedures to prevent, detect, contain, and correct security violations.	**164.308(a)(1)(ii)(A)** - Risk Analysis Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Configure Pulse Profiler to detect and profile all devices within your practice that could be used to access or store ePHI. Based on profile information, determine if there are any vulnerabilities in the operating system that could potentially cause ePHI to be lost or stolen. Review new devices detected by Profiler on a periodic basis - last 24 hours, 7 days or last 30 days.
	164.308(a)(1)(ii)(D) - Information System Activity Review Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Regularly review log-in attempts by scanning PCS/PPS user access logs. Configure PCS/PPS to send logs to a syslog server so that the logs can be analyzed centrally and stored for a longer duration.
164.308(a)(3)(i) - Workforce Security Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a) (4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	**164.308(a)(3)(ii)(A)** - Authorization and/or Supervision Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	User roles should be configured in PCS/PPS to ensure only authorized persons have access to ePHI information.
	164.308(a)(3)(ii)(C) - Termination Procedures Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a) (3) (ii) (B) of this section.	Once a user is removed from the backend authentication server (e.g. AD/LDAP), the device used to access the network is either quarantined, or removed from the network.
164.308(a)(4)(i) - Information Access Management	**164.308(a)(4)(ii)(B)** - Access Authorization Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	Configure PCS/PPS roles and realms to ensure that access is granted to the "right" user with the "right" devices. Also, role-based access control ensures users get access to only those resources for which they authorized.
164.308(a)(5)(i) - Security Awareness and Training Implement a security awareness and training program for all members of its workforce (including management).	**164.308(a)(5)(ii)(c)** - Login Monitoring Procedures for monitoring log-in attempts and reporting discrepancies.	PCS/PPS appliances log all log-in attempts (successful, or unsuccessful) to the event log for review by the admin. You can also use the "Active Users" view in the admin UI to monitor the logins in real time.

Click here to learn more about the Pulse Access suite.

Conclusions

The health care industry is facing tremendous transformation and growth with the increase of intelligent and network enabled medical devices, rise of BYOD for accessing medical information and the need for role based access control to data and applications. The key to support this transformation is to provide HIPAA compliant secured access for these devices and all the users behind them. Secure Access begins with "Visibility", i.e. getting to know all that is present on the network. This must then be followed up by creating rules and policies to ensure only compliant devices are able to access the network, and the rest are placed in a remediation zone.

References

1. HIPAA
   https://www.hhs.gov/hipaa/
2. OCR Breach Portal
   https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
3. The Medical Device Cybersecurity Challenge
   http://www.himss.org/getinvolved/medical-device-cybersecurity-challenge
4. Manhattan Research Report
   http://www.drgdigital.com/h/i/328156200-mobile-rx-info-seeking-is-surging-and-driving-point-of-care-discussions-is- your-brand-ready