HIPAA Considerations for Unified Communications

Abstract: Organizations deploying Unified Communications (UC) in healthcare environments will need to address the security and privacy implications mandated by the HIPAA and HITECH Federal statutes. This white paper discusses these security and privacy issues, and how to configure Polycom UC devices to manage these mandates.

Unified Communications in Healthcare

> *"Polycom video collaboration has literally changed the way we practice medicine. It is patient-centered care in the purest form. Doctors all over the region can provide life-saving services to any cardiac patient in any of our facilities. And by reducing rehospitalizations, our program is driving costs down for patients and other payers."*
>
> **Philip Wolford**
> Coordinator of Saint Vincent's regional telemedicine network

Healthcare organizations the world over are turning to Polycom video collaboration solutions to improve care and reduce cost. Collaborative healthcare solutions from Polycom enable patient centered care, multi-disciplinary team support, reduction of unnecessary re-hospitalizations, and collaboration across the entire healthcare team independent of physical barriers. There are many reasons why eight of the top 10 hospitals and the top ten pharmaceutical companies worldwide are Polycom customers.

"[Multidisciplinary] teams of doctors now collaborate remotely during grand rounds, exchanging observations, recommendations and patient information to improve and accelerate patient care," explained Wolford. These grand rounds are recorded, archived and published for staffers to view later on-demand as part of their continuing medical education.

Telemedicine/Patient Care

> Today's healthcare model requires prevention and wellness programs, and easy access to expert consultations no matter where or when the need arises. Polycom video collaboration solutions enable video collaboration across the healthcare community to support patient centered care, remote consultations, case management, multi-disciplinary teams and collaboration independent of geographic location.

Medical Education

> Whether it's bringing the latest prevention information to the elderly at community health centers or innovative surgical techniques to distant practitioners, Polycom

powers video collaboration for medical education. Today medical education is about multipoint live video for patients and practitioners, and the ability to use Video Content Management solutions from Polycom to record, archive, and make available video content to support healthier patients with fewer un-necessary hospitalizations.

Healthcare Administration

Improve communications and collaboration across the entire healthcare delivery system for better decision-making, project management, efficiency, cost-savings and productivity with Polycom video collaboration solutions.

The HIPAA/HITECH Acts

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress and signed into law in 1996. It aimed to ensure that people changing jobs could "take their insurance with them", as well as encourage the use of electronic medical records. The HIPAA act specifies both privacy and security requirements for these electronic records.

In 2009 Congress enacted the Health Information Technology for Economic and Clinical Health Act (HITECH), allocating nearly $26 Billion to promote the use of information technology in Healthcare. The HITECH act enhanced the HIPAA privacy and security requirements.

Protected Medical Information

Protected Medical Information (PMI) is defined in the HIPAA statute. The two areas of concern are the use of PMI (sharing, utilization, examination, or analysis) and the disclosure of PMI. When you look at the use of UC in a healthcare context, there are two technical security areas that map to the use and disclosure of PMI:

- **Data in Motion**. As data (particularly video) traffic traverses a network from one endpoint to one or more other ones, the data in motion needs to be protected. Encryption is the security technology most helpful here.
- **Data At Rest**. If video is recorded and stored, that stored data needs protection. This is typically done by archiving the data on special servers and using Data Loss Prevention (DLP) products to control access to the data. A number of DLP products are available in the market from a number of vendors, and will not be further addressed here.

The HIPAA Privacy Rule

The HIPAA Privacy Rule regulates the use and disclosure of Protected Medical Information (PMI). PMI includes patient health data, insurance and payment data, and similar data that can be traced back to a particular individual. While PMI can be disclosed without a patient's consent in the normal execution and furtherance of medical treatment, providers are required to take reasonable steps to only release

the minimum necessary information. Failure to take these measures has led to fines and financial settlements[1].

The HIPAA Security Rule

The HIPAA Security Rule specifies administrative, physical, and technical safeguards for PHI, to provide protection against reasonably anticipated threats to the confidentiality, integrity, or availability of electronic PMI. For our purposes, the technical safeguards are most significant when considering UC in a Healthcare environment. Technical safeguards include a wide range of controls:

- Intrusion Prevention, to keep outsiders from capturing PHI from devices or as it flows across a network;
- Data Integrity assurance, to make sure that data has not been unintentionally changed, or changed without authorization;
- Data Corroboration, defining the use of digital signatures and other techniques to ensure that data has not been changed;
- Authentication of communications, to make sure that only authorized parties access PMI; and
- Documentation of device configuration to ensure that systems are configured and controlled in a manner that will appropriately protect PMI.

The HITECH Act provides a provision specifying periodic audits for Healthcare organizations[2].

The good news for Healthcare providers is that the controls listed above are widely available in commercial computing and communications products, and are implemented in Polycom's UC product set. Because the HIPAA Security Rule is by design scalable and flexible – to allow organizations to implement standards as appropriate for their circumstances – security controls and policies can be customized to leverage these security features to tailor a policy to their risk profile. This tailoring of controls can be based on a number of factors:

- The costs of the security measures;
- The likelihood and possible impact of potential risks;
- How security measures will be reviewed and modified in a changing environment.

NIST Publications Define the Security Landscape

The Security Rule calls for "Reasonable and Appropriate" measures to protect PMI, based on their risk analysis. The National Institute of Standards and Technology (NIST) has defined a series of security standards that while are only required for Federal Agencies, are widely considered to be industry Best

[1] University of California settles HIPAA violation case for $865,500. http://www.hhs.gov/news/press/2011pres/07/20110707a.html

[2] SEC. 13411. Audits.

Practice. As such, they provide valuable guidance for implementers and auditors. Two NIST publications in particular are helpful:

- NIST SP 800-30[3] (Guide for Conducting Risk Assessments), which defines risk in terms of the overlap between threats, vulnerabilities, likelihood , and impact; and
- NIST 800-53[4] (Recommended Security Controls for Federal Information Systems and Organizations) which represents best practice in the field.

Note that Polycom's Recommended UC Security Best Practices are based on NIST 800-53[5].

Organizations should keep in mind that the Security Rule is by intent flexible so that organizations can tailor their security policies to their risk profiles. The Polycom UC Security Best Practice recommendations reflect this flexibility, sometimes presenting options in a "Good/Better/Best" format. Healthcare organizations will want to leverage this as they deploy appropriately secure UC systems.

UC Security – Threats, Likelihood, and Mitigation

Polycom UC Products provide a set of security features that can be enabled to address risks to Healthcare systems, as mandated in the Privacy and Security rules and as defined in NIST 800-30 and NIST 800-53.

Firewalls and Firewall Traversal

Every organization has a Firewall which keeps Internet intruders from accessing the organization's computer systems. When deploying UC and video services, mobile users will want to participate in telemedicine from their smartphones, tablets, or mobile laptop computers. This can provide enhanced patient outcomes, for example by allowing remote experts to participate in treatment analysis, enlarging the pool of experts who might be available to help and the hours that they might be available in emergencies.

These remote users need to be able to securely transit the Firewall. Polycom's RealPresence Access Director (RPAD) provides this secure Firewall Traversal. It has been independently evaluated by ICSA Labs, the most prominent 3rd party that tests and certifies firewalls for security[6].

Encryption

Encryption is perhaps the most important consideration to Healthcare organizations addressing HIPAA and HITECH compliance, because it is called out by name in those acts. It is trivial for an

[3] Available at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
[4] Available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
[5] Available at http://www.polycom.com/security
[6] The ICSA security evaluation report for the RPAD is available at https://www.icsalabs.com/sites/default/files/Polycom_RPAD_Final_Evaluation_Report_0.pdf

attacker to silently eavesdrop on data communications crossing a network, recording and PMI that crosses his path. Encryption is a technology that scrambles the transmission such that even if the communications were recorded, the PMI could not be unscrambled.

Polycom UC devices provide the capability of encrypting UC sessions. Polycom provides strong encryption mandated by the US Government's FIPS 140 requirement[7], and while non-Government organizations do not need to comply with FIPS-140 they get the benefit that this testing ensures that only strong encryption ciphers with long key lengths are used. Communications will be protected by AES-128 or AES-256 encryption. If desired, you can configure Polycom devices to force the use of strong encryption. Devices not complying with this will not be able to join the videoconference. This provides "fail safe" encryption to ensure compliance with the HIPAA and HITECH mandates.

Note that Polycom has done extensive optimization of our encryption routines so that there is no performance degradation when encryption is enabled.

Integrity – Authentication, Intrusion Detection

NIST 800-53 recommends that computing devices be "hardened" against attack. Polycom has implemented a series of hardening steps to make our UC devices resistant to external attack:

- All devices are designed to implement security guidance from the US Defense Department's Secure Technical Implementation Guides (STIGS)[8]. We have submitted a number of products for DoD testing and certification to the UCAPL, which includes validation of STIG compliance[9].
- Polycom uses a set of 7 commercial and Open Source vulnerability scanners during the product development and test cycles.
- Some Polycom UC devices include built-in Intrusion Detection technology that detects and alerts in real-time when the devices are under attack.
- Polycom UC devices contain an extensive user authentication capability which can be integrated into an organization's existing Microsoft Active Directory infrastructure.
- The same encryption routines that provide privacy protection for PMI can also provide device authentication, via the use of X.509 certificates, 802.1x network authentication, and the like.

Availability

One key area of security that is particularly applicable to Healthcare is the availability of computing and network resources. As Healthcare organizations become more reliant on the use

[7] Polycom FIPS 140 certificate numbers are available at http://www.polycom.com/solutions/solutions-by-industry/us-federal-government/certification-accreditation.html
[8] Available at http://iase.disa.mil/stigs/
[9] See http://www.polycom.com/solutions/solutions-by-industry/us-federal-government/certification-accreditation.html

of UC to allow access by experts, a system or network outage could become literally a matter of life or death. Polycom provides the industry's best set of technology to ensure "always available" UC platforms:

- The Polycom Distributed Management Application (DMA) allows the virtualization of video meeting room resources. This means that video bridges can be hot-swapped out for maintenance as needed, and that video performance load can be automatically spread across the least loaded systems. End users simply dial their "Virtual Meeting Room" (VMR) number and the system ensures that resources are available to handle the conference.
- The Polycom DMA can provide geographic clustering capabilities that will automatically handle resource allocation even in the event of natural disaster or other wide-spread outage. Even if a data center in New York is not available, the DMA Super-Cluster feature will provide automatic failover to a data center in, say, Kansas City. End users simply dial their same VMR number, and the system will automatically locate the resources to handle the conference.
- Virtualization and performance load "Burst" capability is provided by Polycom's cloud UC product, CloudAXIS. One advantage of virtualized environments is that new virtual instances can be rapidly spun up and brought on line to meet bursts of instantaneous resource demand. Again, users simply dial their VMR number, and the system handles unexpected spikes in demand.

Flexibility

The HIPAA and HITECH Security Rules were intentionally written to be flexible, allowing organizations to adapt their protection profiles to their perceived risks. UC systems must provide corresponding flexibility in how they implement security. Polycom has pioneered a unique capability that allows security to remain flexible, but still ensure that it is deployable and manageable:

- Polycom video endpoints provide a set of built-in Security Levels that pre-configure many individual security features to implement a range of overall security from minimal to very rigorous. Organizations can use one of these "out of the box" if it is a close match to their individual security needs; alternatively, they can use one of these levels as a basis to minor modification to provide an exact match to their security needs.
- Polycom's RealPresence Resource Manager (RPRM) can import a custom security configuration from a Polycom video endpoint and use that as a template to push the same security settings to dozens or hundreds of other endpoints using its "Bundled Provisioning" capability.

Audit

Something that has only begun in the last couple of years is a series of HIPAA audits, where external auditors assess an organization's HIPAA compliance. While there are a large number of

considerations in an audit, security technical controls should provide easy reporting to auditors. Polycom provides a number of capabilities that simplifies any technical security audit:

- Polycom uses industry-standard logging technology, allowing UC devices to send security events to a central Syslog data collector (or Security Information Manager) for correlation, analysis, and reporting.
- Polycom's HDX video endpoint includes a Configuration Audit in its Support Package. This configuration audit captures the instantaneous security configuration settings in an industry standard format (Security Configuration Automation Protocol, or SCAP[10]), allowing HIPAA compliance analysis via industry standard SCAP reporting tools. Even if your organization has a large number of HDX endpoints, it will be short work to collect a support package from each one and run a report for it. Polycom is the only UC vendor providing an automated HIPAA compliance reporting capability.

Summary

HIPAA and HITECH bring a lot of administrative complexity to Healthcare IT. UC and videoconferencing is new, and it's important that complexity is not layered on complexity. While there cannot be a "HIPAA in a box" solution, Polycom has leveraged existing industry standards and best practices to provide a HIPAA UC technical framework that is flexible, manageable, and auditable.

[10] See http://scap.nist.gov/