



Remote Access to a Healthcare Facility and the IT Professional's Obligations under HIPAA and the HITECH Act

Are your Authentication, Access, and Audit Paradigms up to date?

A White Paper

By Kerry Armstrong, Privacy,
Risk & Compliance, Picis, Inc.
&
SecureLink, Inc.

Synopsis

Recent legislation is providing renewed emphasis on HIPAA's privacy and security requirements as well as resources to identify and punish covered entities and their business associates for non compliance. Savvy healthcare IT professionals and Privacy Officers are revisiting their policies and procedures to ensure HIPAA compliance. Remote access to a healthcare facility's networks and systems is an often overlooked area that can represent significant potential exposure for HIPAA breaches. With the right tools and procedures, however, remote access risks can be largely eliminated and HIPAA compliance documented.

HIPAA and the IT Professional

It's been more than 10 years since the Health Insurance Portability and Accountability Act (HIPAA) was enacted. Since that time, Healthcare Facility operations have evolved to rely on software and technology to a much greater degree. Larger, faster networks, more complex software, and more instances of software inside a healthcare facility's network seem to be the norm. As a result, healthcare IT departments have had to become smarter and their practices have had to evolve.

Now, new legislation is bringing renewed emphasis to HIPAA and its requirements. The Health Information Technology for Economic and Clinical Health Act (HITECH) a subset of the American Reinvestment and Recovery Act (ARRA) provides funding for healthcare facilities and providers to utilize electronic health records and drive efficiencies into the healthcare system. As EHRs drive automation and interoperability into the healthcare system, the importance of privacy and security of those records heightens, so ARRA also provided additional accountability. Beginning this year, the Secretary of Health and Human Services is required to report to Congress the number of HIPAA audits conducted and the nature of the findings. As a result, covered entities such as hospitals, doctors, and health plans as well as business associates (vendors of covered entities that gain access to PHI in the course of their business arrangements) can expect to be audited. The fines are substantial and can range up to \$1.5 million in a calendar year. Criminal liability can result in fines of \$250,000 and up to 10 years in prison. In other words, HIPAA now has teeth.

HIPAA has several goals, however Title 2, which addresses protection of an individual's health information against access without consent or authorization - safeguarding Protected Health Information (PHI) - is probably of most consequence to Privacy Officers and IT professionals working in healthcare facilities. Since PHI resides throughout a healthcare facility's network, it is the healthcare IT professional's duty to ensure that the networks, databases, and systems they oversee support HIPAA compliance, including access to those networks, databases, and systems. HIPAA, 45 CFR Parts 164.306(a) and 164.308(a).¹

It is access to those networks, databases, and systems - specifically remote access - that is the subject of this White Paper. Since remote service and support of complex software and systems is a fact of life for most healthcare IT departments, the professionals in those departments must take care to ensure the manner in which their software and systems is accessed for remote support is HIPAA compliant. As every competent healthcare IT professional knows, policies, procedures and access methods that may have been more than adequate a few years ago, may not be sufficient today.

Remote Support & Security and Privacy

HIPAA requires Administrative, Physical and Technical Safeguards that are outlined in various Standards and Implementation Specification Guidelines. Some of these safeguards (relevant to the topic of this whitepaper) mandate basic requirements for security and privacy as it relates to PHI access,² including:

- Identification and authentication
- Limiting access, including terminated users
- Audit controls, and
- Secure data transfer (Integrity)

HIPAA requires the same level of security and privacy safeguards whether the service engineer is servicing the software onsite or accessing the application remotely. Fortunately, SecureLink™ remote support networks

¹ HIPAA requires healthcare providers to "ensure the confidentiality, integrity, and availability of all electronic [PHI]" and to assess risks "to the confidentiality, integrity, and availability of electronic [PHI]." 45 CFR Parts 164.306(a) and 164.308(a).

² See Generally HIPAA, 45 CFR Part 164; see also *Security and Privacy Requirements for Remote Servicing*, Joint NEMA/COCIR/JIRA Security and Privacy Committee (Nov. 2001).

(SecureLink) make the healthcare IT professional's job easier by enabling secure, effective remote access that supports HIPAA Compliance. Let's look at each security requirement more closely.

1. Identification and Authentication

It is fundamental that healthcare facility IT personnel know who is accessing their network, software, and systems, and that the person or entity gaining access is the one claimed. HIPAA, 45 CFR Part 164.312(d).³ Many hospitals allow vendors to access their systems via shared user IDs (or can't determine whether this is occurring or not). This is a direct violation of HIPAA, as HIPAA requires the use of unique user IDs. Although the hospital may know that a particular vendor has accessed their system, there may be hundreds of customer support representatives all sharing multiple user IDs without any accountability at the individual level.. This common process needs to change in order to meet HIPAA and HITECH Act mandates.

- > SecureLink employs dual factor authentication. First, both the service engineer and the healthcare IT professional have a unique username and password. SecureLink also enforces restrictive password requirements for all users. Finally, every secure connection requires a randomly generated, single use, temporary key that must match on both sides of the connection.⁴ A healthcare facility can also limit access to a range of IP addresses or authorized networks.

2. Restricting Access

A robust, remote access solution that supports HIPAA compliance should grant a remote service engineer as much access as needed, but also allow a healthcare facility IT professional to limit the engineer's access to only those parts of the software or network that are required to resolve the immediate service issue. HIPAA, 45 CFR Part 164.312(a).⁵ HIPAA also requires that a covered entities' workforce without authorized access to PHI be restricted from accessing it. HIPAA, 45 CFR 164.308(a)(3)(i). In addition, a remote access solution should address procedures for terminating access to PHI when the employment of a workforce member ends or as otherwise required by the Act. HIPAA, 45 CFR 164.308(a)(3)(ii)(C). (Potentially impossible in the case of shared user IDs).

- > SecureLink is customer configurable to grant and restrict access. The healthcare facility IT professional is in control. SecureLink provides powerful, direct to server access, but a remote service engineer's access can also be limited as to time and scope and as granularly as access to a single port. In addition, access rights can be restricted based on user groups or security clearances. SecureLink works seamlessly with existing security protocols; the networks require no modification to the firewall. SecureLink allows a hospital to mask logon credentials (helpful in preventing terminated business associate employees from gaining access), and it also integrates with Active Directory system for timely removal of terminated users.

3. Audit Controls

Creating an audit record is part of any sound security policy. Accordingly, a healthcare IT professional will want to create, store, and protect appropriate log files of all security sensitive activities that take place during a remote session. HIPAA, 45 CFR Part 164.312(b).⁶ In addition, HIPAA requires a covered entity "to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." HIPAA, 45 CFR 164.308 (a)(1)(ii)(D). Under the HITECH Act, a patient can request a disclosure accounting from a covered entity basically asking "who has viewed my health information" for up to the prior 3 years. HIPAA, 45 CFR 164.528(a) and HITECH Act, 13405(c). A covered entity should be prepared to respond to such patient accounting requests.

- > In addition to real time monitoring and unilateral session termination rights, SecureLink provides high definition audit reports of each remote session including detailed log files and video capture of screen sharing or RDP sessions if desktop access has occurred. The reports identify who accessed the system and when, what areas were accessed, what was done (at the command

³ HIPAA requires that healthcare providers "[i]mplement procedures to ensure that the person or entity seeking access ... is the one claimed." 45 CFR Part 164.312(d).

⁴ This key can be configured to allow anytime access to trusted vendors.

⁵ HIPAA requires that healthcare providers "allow access only to those person or software programs that have been granted access rights." 45 CFR Part 164.312(a).

⁶ HIPAA requires healthcare providers to "record and examine activity in information systems that contain or use [PHI]." 45 CFR Part 164.312(b).

level), what tools were used, who authorized access, the reason for access, and the case number. SecureLink also provides an audit trail of log on attempts. HIPAA, 45 CFR 164.308(a)(5)(ii)(C).

4. Secure Data Transfer

All data transferred between the Healthcare Facility and the remote service center must be treated as confidential unless there is a legal certainty that the data contains no PHI. HIPAA, 45 CFR Part 164.312(e)(2).⁷

- > SecureLink offers customer configurable levels of encryption, up to and including 3DES, Blowfish, 192-bit AES, or 256-bit AES encryption.

SecureLink™ Remote Support Networks Summary

HIPAA Requirement	SecureLink Feature
Identification & Authentication	Dual factor, unique user name and password controls Restrictive password requirements Randomly generated, one time use keys Grant access only to customer authorized networks
Restricted Access	Customer configurable Restrict access as to time and scope, down to file level Access rights can be restricted at system or user level Ability to mask logon credentials Integration with Active Directory
Audit Controls	Real time monitoring High definition audit reports Detailed log files, video capture of screen sharing/RDP sessions Unilateral ability to terminate session at any time
Secure Data Transfer	Customer configurable levels of encryption, up to and including, 3DES, Blowfish, and 256 AES

Conclusion

Although HIPAA has been on the books for over a decade, its enforcement was generally seen as lax, and compliance with its requirements often took a back seat to more pressing issues – technological and otherwise - within a healthcare facility. Now that the HITECH Act has been enacted, hospitals, healthcare providers and their business associates are being forced to take another look at how they have been doing business. With HIPAA audits forthcoming, HIPAA requirements are moving to the forefront.

As technology is continually being used to drive efficiencies into the healthcare system, the potential for electronic breaches, unintentional or otherwise, increase exponentially. Proactive healthcare IT professionals will examine the way they are doing things and make changes where necessary. Those that don't change, risk falling behind or worse. Let's face it, healthcare technology is not only here to stay, but destined to expand at an increasing rate along with the regulatory framework that governs it.

Although satisfying HIPAA compliance requirements in the context of ever changing, increasingly complex healthcare IT operations can add additional stress to overworked healthcare IT departments, SecureLink can help. As a secure, effective answer to concerns about a HIPAA compliant remote support solution, SecureLink remote support networks allow healthcare IT professionals to spend less time concerned with securing remote access and more time on IT operations.

⁷ HIPAA requires healthcare providers to “encrypt electronic [PHI] whenever deemed appropriate.” 45 CFR Part 164(e)(2).

About Kerry Armstrong

Kerry Armstrong is responsible for Privacy, Risk & Compliance for Picis, Inc, a global provider of innovative information solutions that enable rapid and sustained delivery of clinical, financial and operational results in the acute care areas of the hospital— emergency department (ED), operating rooms (ORs), post-anesthesia care units (PACUs) and intensive care units (ICUs).

Kerry leverages her 18 years of technical expertise to provide Picis and its clients guidance on security, privacy, and compliance challenges. She serves as a trusted business advisor to her customers. Kerry provides critical tactical solutions to Picis and its customers facing increased regulation including timely issues such as MA privacy compliance, and HIPAA / HITECH Act compliance.

She has deep knowledge in the areas of risk assessment, general computing controls, and business processes from both a technical and financial standpoint. Prior to joining Picis, Kerry held various positions at the Gillette Company, Arthur Andersen, B.J. Wholesale Club, Inc, and most recently Vice President IT Risk & Compliance for Caturano and Company.

About SecureLink

SecureLink™ is an Austin-based provider of secure networks for complex remote support. SecureLink remote support networks are specifically designed to enable effective, remote service and support to server-based software in secure, regulated environments. Visit us at www.securelink.com or email us at info@securelink.com. 1715 S. Capital of Texas Hwy, Suite 100, Austin, Texas 78746.