SECURELINK

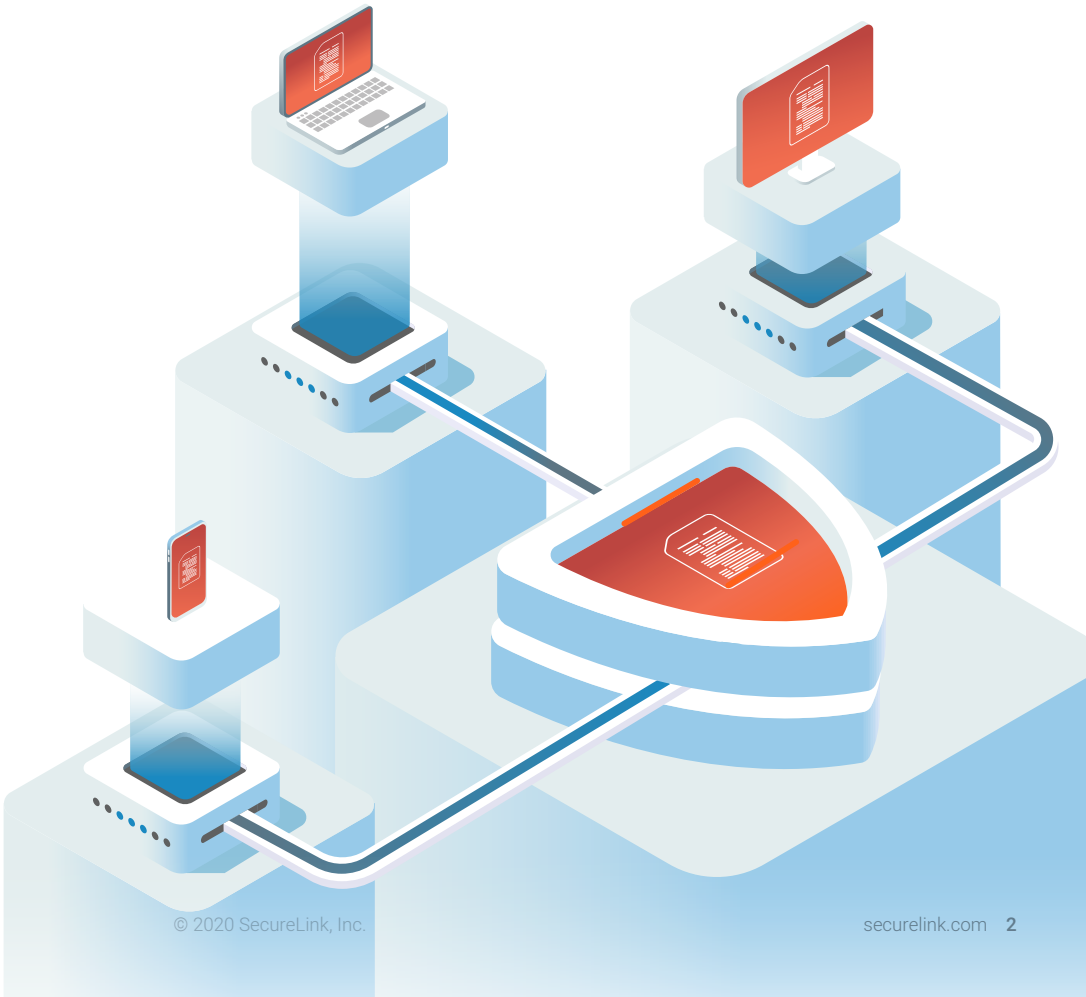
HIPAA and HITECH Requirements for Remote Access to a Healthcare Facility

Are your authentication, access, and audit controls up to date?

HIPAA and HITECH Requirements for Remote Access to a Healthcare Facility

Are your authentication, access, and audit controls up to date?

TABLE OF CONTENTS



© 2020 SecureLink, Inc.

SYNOPSIS

The HITECH update to HIPAA legislation provides a renewed emphasis on HIPAA's privacy and security requirements and offers resources to identify and punish covered entities and their business associates for noncompliance. Savvy healthcare IT professionals and Compliance Officers are revisiting their policies and procedures to ensure HIPAA and HITECH compliance. Remote access to a healthcare facility's networks and systems is an often overlooked area that can represent significant potential exposure for HIPAA violations. With the right tools and procedures, however, remote access risks can be greatly reduced and HIPAA compliance documented.

HIPAA AND THE IT PROFESSIONAL

It's been decades since HIPAA was passed and over a decade since the HITECH update, and 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.

> 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 for Healthcare makes the IT professional's job easier by enabling secure, effective remote access that supports HIPAA/HITECH compliance. Let's look at each security requirement more closely.

HITECH legislation is bringing renewed emphasis to HIPAA and its requirements. As a subset of the American Reinvestment and Recovery Act (ARRA), HITECH provides funding for healthcare facilities and providers to utilize electronic health records (EHR) and introduce efficiencies into the healthcare system. As EHRs continue to drive automation and interoperability into the healthcare system, the importance of privacy and security of those records increases, so ARRA also required additional accountability. The HITECH Act requires the Secretary of Health and Human Services is required to report covered entities such as hospitals, doctors, and health plans as well as business associates (vendors of covered entities that gain access to personal health information (PHI) in the course of doing business) are all audited. The fines for violations 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 gained teeth. To date, the Office of Civil Rights (OCR), the enforcement arm of HHS for HIPAA and HITECH, has assessed over $110,000,000 in fines.

© 2020 SecureLink, Inc.

HIPAA has several goals, including the mandating of portability of medical records; however, Title 2 is probably of most consequence to IT and Privacy Officers. This section addresses the protection of an individual's PHI against access without authorization or consent. 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 that they oversee support HIPAA compliance, including access to those networks, databases, and systems. [See HIPAA 45 CFR Parts, 164.306(a), 164.308(a)].

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 that 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.

IDENTIFICATION AND AUTHENTICATION

It's 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 who is authorized. [See HIPAA, 45 CFR Part 164.312(d).3]. Many hospitals allow vendors to access their systems via shared user IDs. This is a direct violation of HIPAA and HITECH, as they require 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 end in order to meet HIPAA and HITECH mandates.

SecureLink for Healthcare employs multi-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. A healthcare facility can also limit access to a range of IP addresses or authorized networks.

RESTRICTING ACCESS

A robust remote access solution that supports HIPAA compliance should grant only as much access that is needed by limiting access to only those parts of the software or network that are required to resolve the immediate service issue. [See HIPAA, 45 CFR Part 164.312(a).5]. HIPAA also requires that organizations restrict workforce access to PHI to only those who are authorized. [See 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 [See HIPAA, 45 CFR 164.308(a)(3)(ii)(C)].

SecureLink for Healthcare is customer configurable to grant and restrict access. The healthcare facility IT professional is in control. SecureLink for Healthcare 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

© 2020 SecureLink, Inc.

to a single port. In addition, access rights can be restricted based on user groups or security clearances. SecureLink for Healthcare works seamlessly with existing security protocols; the networks require no modification to the firewall. SecureLink for Healthcare allows a hospital to mask logon credentials (helpful in preventing terminated business associate employees from gaining access), and it also integrates with Active Directory systems for timely removal of terminated users.

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 [See 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." [See 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. [See 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 for Healthcare 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 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. [See HIPAA, 45 CFR 164.308(a)(5)(ii)(C).].

SECURE DATA TRANSFER

All data transferred between a healthcare facility and a remote vendor must be treated as confidential unless there is a legal certainty that the data contains no PHI [See HIPAA, 45 CFR Part 164.312(e)(2).7].

SecureLink for Healthcare offers customer configurable levels of encryption, up to and including 3DES, Blowfish, 192-bit AES, or 256-bit AES encryption. (ii)(C)].

Remote Access, Security, and Privacy

HIPAA requires administrative, physical, and technical safeguards that are outlined in various standards and implementation specification guidelines. Some of these safeguards mandate basic requirements for security and privacy as it relates to PHI access, including:

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

© 2020 SecureLink, Inc.

SecureLink for Healthcare Summary

HIPAA REQUIREMENT	SECURELINK FOR HEALTHCARE FEATURE
Identification & Authentication	• Multi-factor authentication, support for SMS and TOTP • Unique username 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 • Active Directory integration
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, AES 128, 192, and 256 bit modes

CONCLUSION

Though HIPAA has been in effect since 2005, 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. With the enactment of HITECH and the exploitation of healthcare providers via ransomware and other real threats dramatically increasing the stakes of noncompliance, hospitals, healthcare providers and their business associates are forced to take another look at how they have been doing business.

As technology continues 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, HIPAA citations and fines, or worse, data breaches of confidential patient data. Healthcare

© 2020 SecureLink, Inc.

technology is not only here to stay, but destined to expand at an increasing rate along with the regulatory framework that governs it; new state and local regulations add to the compliance burden around data security.

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 for Healthcare can help. As a secure, effective answer to concerns about a HIPAA compliant remote access solution, SecureLink for Healthcare allows healthcare IT professionals to spend less time concerned with securing remote access and more time on IT operations.

ABOUT SECURELINK

SecureLink is the leader in managing secure vendor privileged access and remote support for both highly regulated enterprise organizations and technology vendors. More than 30,000 organizations across multiple industries including healthcare, financial services, legal, gaming, and retail rely on SecureLink's secure, purpose-built platform. SecureLink is headquartered in Austin, Texas.

For more information please visit securelink.com or call us at 1.888.897.4498