HIPAA and HITECH

SECURELINK

Mitigating Risks of HIPAA Noncompliance

About 56% of provider organizations have already experienced a vendor or third-party breach.[1]

Detailed Audit Trails

Healthcare organizations are required to demonstrate an increasing level of visibility and control around their vendors' activity to maintain compliance with these mandatory standards.

About privileged remote access for HIPAA and HITECH

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) outline the standards and requirements for the assurance of confidentiality, integrity, and availability of personal health information (PHI). These requirements aren't just for healthcare providers and organizations, but their business associates, too. **In other words, anyone who touches PHI must follow the requirements laid out. If not, they face the potential legal liability for noncompliance.**

A component of HIPAA, the Security Rule, was implemented to ensure the confidentiality, integrity, and availability specifically of electronic PHI (ePHI), and details the standards to protect that information via administrative, physical, and technical safeguards. **Healthcare enterprises and their business associates need to follow these rules if they have any access to, or if they transmit, personal health data.**

SecureLink provides the means to mitigate the risk of HIPAA noncompliance posed by your third-party vendors. With granular control over vendor access to your networks, as well as detailed audit trails to log all third-party activity, SecureLink will be a valued partner in helping you meet your compliance requirements.

With this, healthcare organizations are required to demonstrate an increasing level of visibility and control around their vendors' activity to maintain compliance with these mandatory standards.

Remote access tools, such as VPNs or desktop sharing, often do not meet the standards required to pass an internal or Office of Civil Rights audit. On top of that, vendors accessing your network provide a weak point that dramatically increases the risk of a security breach. In fact, according to Health IT Security, about 56% of provider organizations have already experienced a vendor or third-party breach.[1]

1 Third-party vendors behind 20% of healthcare data breaches in 2018

Why over 1,000 hospitals trust SecureLink

HIPAA and HITECH Requirements	SecureLink features	Compliance requirements
GENERAL SECURITY RULES	• SecureLink restricts access to systems with ePHI down to the vendor or vendor rep level and can require pre-approval prior to access • SecureLink is built specifically to protect against threats to the security of ePHI by mitigating unauthorized third-party access and auditing all activity	• Ensure the confidentiality, integrity, and availability of ePHI • Protect against reasonably anticipated threats • Business associates must implement security measures to abide by these standards
ADMINISTRATIVE SAFEGUARDS	• Vendors are given role-based least privileged access with granular permission controls • SecureLink provides flexible workflows, configurations, and security settings specific to the risk analysis of third parties • SecureLink streamlines the authorization process with vendor self-registration, built-in multi-factor authentication, and audited access request workflows	• Implement security measures to reduce risks to ePHI • Allow access to ePHI only when access is appropriate based on user role • Periodically assess risk, disaster recovery, and security procedures
TECHNICAL SAFEGUARDS	• SecureLink offers a detailed audit of all vendor access and activity, including HD video and keystroke logs at the individual user and session levels • SecureLink provides vendor employment verification and granular automatic and manual controls over vendor access • Audit data at rest is encrypted at 256-bit AES	• Implement procedures that only allow access to authorized persons • Record access and activity and examine audit trails • Ensure that ePHI is not improperly altered or destroyed • Guard against unauthorized access to ePHI that is transmitted over a network

Risks of getting privileged remote access wrong

Fines[1]

Healthcare data breach costs:

Average cost per healthcare record is $408.

Average cost of a breach is $3.86 million.

Lost money and reputation[3]

Post-breach, the average share value dropped by 5%.

31% of consumers said they would discontinue their relationship after a breach.

65% reported a loss of trust with organizations that suffered one or more data breaches.

Vendor risk[4]

Over 20% of data breaches in the healthcare sector in 2018 were from organizations working with third-party vendors.

Third-party vendors working with healthcare provider organizations are responsible for some of the largest healthcare data breaches to date.

23% of the vendors assessed represented a medium-to-high risk to healthcare organizations.

Patient safety[2]

The #1 patient safety risk in 2019 is that hackers can exploit remote access to systems, disrupting healthcare 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.

CONTACT US:
securelink.com
888.897.4498
contact@securelink.com

1 Common HIPAA violations 2 Data hazards in 2019 3 Data breaches and reputation 4 Third-party vendors behind 20% of healthcare data breaches in 2018