imprivata®

ENTERPRISE ACCESS

The Third-Party remote access solution for HIPAA compliance

Cost of a healthcare data breach

The average cost of a data breach for a healthcare organization is $9.23 million.

Third parties are your weakest attack vector

of healthcare organizations have experienced one or more data breaches caused by a third party.

HIPAA and HITECH requirements for critical remote access

The Health Insurance Portability and Accountability Act (HIPAA) was designed to protect individuals' private health information, while also ensuring that health information is accessible in order to provide appropriate and high-quality care for patients. It outlines the standards for ensuring the confidentiality, integrity, and availability of personal health information (PHI).

The Health Information Technology for Economic and Clinical Health Act (HITECH), enacted several years after HIPAA, included business associates as liable under HIPAA and increased the penalties for non-compliance with HIPAA's Security and Privacy Rules. In other words, anyone who has access to PHI in some way must comply with HIPAA. If not, they face legal liability, fines, and possibly civil and/or criminal penalties for violations.

SecureLink's Enterprise Access provides the means to meet your HIPAA compliance requirements with regards to your third parties' access. With individual identity management, granular control over vendor access, and detailed audit trails that log all activity, SecureLink will be a valued partner in helping you mitigate the risks of non-compliance and increase your third-party security.

The HIPAA Security Rule specifically outlines the physical, administrative, and technical safeguards organizations need to protect and secure electronic PHI (ePHI). While there is flexibility in how organizations implement these safeguards, both healthcare enterprises and their business associates must follow these rules if they have any access to or transmit personal health data.

The Security Rule requires healthcare organizations to maintain compliance by demonstrating a high level of visibility and control around their business associates' access to critical systems and patient data. Traditional remote access tools, such as VPNs or desktop sharing, do not meet the safeguard standards required to pass an internal or Office of Civil Rights (OCR) audit. They are not designed to restrict access to only authorized users, nor do they provide visibility through recordings of access activity for review and examination.

There's a good reason these HIPAA and HITECH requirements are in place -- vendors remotely accessing a healthcare organization's network and clinical applications create vulnerabilities that dramatically increase the risk of a data breach. In fact, 44% of healthcare and pharmaceutical organizations experienced a third-party breach in the past year alone, most often due to granting too much privileged access.

How SecureLink's Enterprise Access enables organizations to meet HIPAA compliance

HIPAA and HITECH Requirements	How Enterprise Access helps organizations	Compliance requirements
GENERAL SECURITY RULES	• Restricts and monitors access of third parties to systems with ePHI • Identify and protect against reasonably anticipated threats • Increases security and protects against anticipated third-party threats when enforced as the required remote access method for all business associates • Provides documentation of third-party remote access procedures and workflows	• Ensure the confidentiality, integrity, and availability of ePHI • Identify and protect against reasonably anticipated threats • Business associates must implement security measures to abide by these standards • Document and maintain policies and procedures to comply with security provisions
ADMINISTRATIVE SAFEGUARDS	• Provides flexible workflows, configurations, and security settings specific to the risk analysis of each vendor • Prevent all unauthorized third parties from accessing ePHI, with zero trust, least privileged access defined by user-role, and down to the host and port level • Streamlines the authorization process with multi-factor authentication and audited access request workflows • Provides audit logs of all activity by individual user sessions—reports on all access, and provides a summary of activity for each session	• Identify and analyze risks to ePHI and implement security measures to reduce risks • Allow access to ePHI only when access is appropriate based on user role and prevent unauthorized access • Periodically assess risk and security procedures against the requirements of the Security Rule • Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports
TECHNICAL SAFEGUARDS	• Enforces use of individual user accounts and verifies current employment status and identities with multi-factor authentication • Defines access on a per-user basis, with configurable access approval workflows • Defines access down the host, port, and service level, preventing access by unauthorized persons • Records detailed audit of all individual vendor activity, including HD video and text logging, to examine activity and integrity of ePHI • Audit data at rest is encrypted at 256-bit AES	• Implement technical procedures that only allow access to ePHI to authorized persons • Record access and activity and examine audit trails • Ensure that ePHI is not improperly altered or destroyed • Verify that a person or entity seeking access to electronic protected health information is the one claimed • Guard against unauthorized access to ePHI that is transmitted over a network

Consequences of non-compliance and a third-party data breach

Risks with third parties

60% of healthcare organizations have experienced one or more data breaches caused by a third party

Just 41% of healthcare organizations have a comprehensive inventory of all third parties with access to their network

Only 44% of organizations rate the effectiveness of their third parties in achieving compliance with their security and privacy regulations as very high

Two thirds (63%) of organizations see third-party remote access to their network becoming their weakest attack surface

Lost revenue and patients

The healthcare industry has the highest industry average cost of a data breach at $9.23 million per breach

Hospitals spend 64% more on advertising after a data breach in an effort to repair the hospital's image and minimize patient loss to competitors

Costs of non-compliance with HIPAA:

Civil violations range from $100 per violation, up to $50,000 per violation, depending on the severity

Criminal violations range anywhere from $50,000 to $250,000 in fines, along with possible imprisonment

Impacts to patient safety after an attack

22% of healthcare organizations report increased mortality rates

70% of healthcare organizations report delays in procedures and tests that result in poor outcomes

71% of healthcare organizations report that patients have longer lengths of stay

Unsecured third-party remote access can end in severe consequences, such as HIPAA penalties, loss of customers and revenue, and direct impacts on patient care and privacy. SecureLink's Enterprise Access secures your third-party remote access risks and enables you to implement administrative and technical safeguards for HIPAA compliance.

Contact us to learn more about how **Enterprise Access** can help.

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com