aspera
an IBM® company

Leverage Aspera to Achieve HIPAA Compliance

SUMMARY

Aspera software products provide security and encryption technologies that organizations need to meet the security requirements of HIPAA. Aspera software ensures secure authentication, data integrity verification, access control and detailed tracking and reporting tools to help organizations protect personal health information and meet HIPAA compliance requirements.

DETAIL

The Health Insurance Portability Act (HIPAA) Privacy Rule establishes, a set of national standards for the protection of certain personal health information (PHI) while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. It provides federal protections for individually identifiable PHI held by covered entities and their business associates and gives patients an array of rights with respect to that information.

The HIPAA Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information (EPHI).

In general, the Privacy Rule sets the standards for who may have access to PHI, while the Security Rule sets the standards for ensuring that only those who should have access to EPHI will actually have access.

COVERED ENTITIES

- Health Plans, Health Care Providers, Health Care Clearing Houses, Business Associates of the covered entities

NON-COVERED ENTITIES

- Life Insurers, Employers, Workers compensation carriers, Schools and school districts, Many state agencies like child protective service agencies, Law enforcement agencies, Municipal offices

PROTECTED INFORMATION

- Any individually identifiable PHI held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral

KEY REQUIREMENTS FOR COVERED ENTITIES:

- Reasonably limit uses and disclosures of PHI to the minimum necessary to accomplish the intended purpose
- Protect sensitive confidential information when sharing data that contains PHI
- Ensure that only intended information is shared or exchanged, and no PHI is disclosed improperly
- Limit who can view and access PHI as well as implement training programs for employees about how to protect it

ASPERA SUPPORTS HIPAA SECURITY RULE

Aspera provides software products with the technical safeguards that can be used by a covered entity to ensure HIPAA compliance. Specifically, the ability to protect EPHI and control access to it.

Read on to learn how Aspera supports the key technical safeguards of Access Control, Audit Controls, Integrity, Person or Entity Authentication and Transmission Security.

Access Control – The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Aspera software supports this rule by providing the following features:

- Authenticated system access with unique user identification
- Automatic logoff after a predetermined time of inactivity
- Respect the file system permissions for the authorized user
- A security model that requires specifically granted access by an administrator
- Encryption and decryption, both over the wire and for any data stored at rest
- Information encrypted with a key can only be decrypted with the same digital key

Audit Controls – Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Aspera software supports this rule by providing the following features:

- Activity is logged to a repository and available via standard and custom reports
- Reports can be viewed to examine activity or to determine if a violation occurred

Integrity – The property that data or information have not been altered or destroyed in an unauthorized manner. All Aspera products support this rule:

- Data integrity verification is performed on each transmitted data block and transfers preserve the native file system access control attributes between all supported operating systems

Person or Entity Authentication – Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Aspera software supports this rule by providing the following features:

- Require authenticated access with unique user identification
- Automatic logoff after a predetermined time of inactivity
- Support for 3rd party directory services such as LDAP, Active Directory and SAML

Transmission Security – Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Aspera software supports this rule by providing the following features:

- Data integrity verification is performed on each transmitted data block and transfers preserve the native file system access control attributes between all supported operating systems
- Encryption and decryption, both over the wire and for any data stored at rest. Information encrypted with a key can only be decrypted with the same digital key