Kiteworks

COMPLIANCE BRIEF

Achieving HIPAA Compliance With Kiteworks

Secure Content Collaboration and Communication for Healthcare Organizations

In the healthcare industry, maintaining the privacy and security of sensitive information is critical. The Health Insurance Portability and Accountability Act (HIPAA) sets forth comprehensive standards to protect the privacy of patient information, known as protected health information (PHI), and to ensure the secure exchange of electronic health information. Achieving and maintaining HIPAA compliance is essential for healthcare organizations, and Kiteworks offers a robust solution for secure content collaboration and communication that can support your compliance efforts.

Privacy Rule Compliance With Kiteworks

Access Controls

The HIPAA Privacy Rule requires covered entities to implement policies and procedures to limit the use and disclosure of PHI to the minimum necessary. Kiteworks supports this requirement by providing granular access controls that enable organizations to manage user permissions at the file and folder levels, ensuring that only authorized users have access to PHI. The platform also offers role-based access controls, allowing organizations to assign specific access rights to users based on their job functions and responsibilities.

Audit Controls

Covered entities are required to have audit controls in place to track and monitor access to PHI. Kiteworks offers comprehensive auditing and reporting capabilities that provide organizations with detailed information about user activities, including file access, sharing, and modification. This level of visibility helps organizations identify potential security risks and demonstrate compliance with the Privacy Rule.

Data Backup and Recovery

HIPAA requires covered entities to have a data backup and recovery plan to ensure the availability and integrity of PHI. Kiteworks offers secure and reliable data backup solutions, with data stored in redundant, geographically distributed data centers. In the event of data loss or system failure, Kiteworks enables organizations to quickly recover their PHI, ensuring continuity of operations and compliance with the Privacy Rule.

Security Rule Compliance With Kiteworks

Administrative Safeguards

Kiteworks helps healthcare organizations meet the administrative safeguards requirements of the HIPAA Security Rule by providing a centralized platform for managing user access and permissions, as well as tools for monitoring and reporting on user activities. Additionally, Kiteworks supports the development and implementation of security policies and procedures, helping organizations create a comprehensive security program that addresses the unique risks associated with handling PHI.

Physical Safeguards

While physical safeguards may not directly apply to Kiteworks as a software solution, the platform supports compliance with these requirements by enabling secure remote access to PHI. With Kiteworks, authorized users can securely access and collaborate on PHI from any device or location, reducing the risk of unauthorized access or theft that can result from storing sensitive information on physical devices.

Technical Safeguards

Kiteworks provides a range of technical safeguards to help healthcare organizations protect their PHI, including:

- **Access Controls.** Kiteworks enables organizations to implement strong authentication and authorization mechanisms, ensuring that only authorized users have access to PHI. This includes the use of multi-factor authentication, single sign-on (SSO) integration, and granular access controls based on user roles and responsibilities.
- **Audit Controls.** Kiteworks offers comprehensive auditing and reporting capabilities that help organizations track and monitor user activities related to PHI. This level of visibility is critical for identifying potential security risks and demonstrating compliance with the Security Rule.
- **Integrity Controls.** To protect the integrity of PHI, Kiteworks offers features such as version control, file locking, and automated workflows that ensure only authorized users can make changes to sensitive information. In addition, the platform provides real-time notifications and alerts to keep users informed of changes to PHI, helping to maintain data integrity.
- **Transmission Security.** Kiteworks ensures the secure transmission of PHI by using encryption for data in transit and at rest. The platform supports industry-standard encryption protocols, such as SSL/TLS for data in transit and AES-256 for data at rest. By encrypting PHI, Kiteworks helps healthcare organizations protect sensitive information from unauthorized access and comply with the Security Rule's transmission security requirements.

Breach Notification Rule Compliance With Kiteworks

Incident Detection and Response

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, the Department of Health and Human Services (HHS), and in some cases, the media, in the event of a breach involving unsecured PHI. Kiteworks supports compliance with this rule by providing advanced security features and monitoring tools that help organizations detect and respond to potential security incidents.

With real-time notifications and alerts, as well as comprehensive auditing and reporting capabilities, Kiteworks enables organizations to quickly identify and investigate potential breaches, minimizing the impact of any unauthorized access or disclosure of PHI.

Omnibus Rule Compliance With Kiteworks

Business Associate Liability

The Omnibus Rule extends the direct application of the Privacy and Security Rules to business associates and their subcontractors, making them liable for compliance and subject to penalties for violations. Kiteworks can facilitate secure communication and file sharing between covered entities and business associates, supporting their compliance efforts.

By providing a secure platform for exchanging sensitive information, Kiteworks helps healthcare organizations and their business associates ensure that PHI is protected and that both parties are meeting their obligations under the Omnibus Rule.

Final Rule for GINA Compliance With Kiteworks

Genetic Information

The Final Rule for the Genetic Information Nondiscrimination Act (GINA) extends the Privacy Rule's protections to genetic information, treating it as PHI. Kiteworks can implement content-defined zero-trust policies to ensure limited access to sensitive genetic information, protecting it from unauthorized use or disclosure. By providing granular access controls and secure communication channels, Kiteworks enables healthcare organizations to manage and protect genetic information in accordance with GINA and the Privacy Rule, ensuring compliance with these important regulations.

Achieving HIPAA compliance is a critical requirement for healthcare organizations, and Kiteworks offers a comprehensive solution for secure content collaboration and communication that can support your efforts. With robust features designed to address the unique challenges of handling PHI, Kiteworks enables healthcare organizations to protect sensitive information, meet regulatory requirements, and provide the highest level of care to their patients.