Olympic IT Services Sentinel+ Managed Backup System

HIPAA COMPLIANCE

HIPAA Overview

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law in 1996 to improve insurance portability (Title I), as well as to reduce fraud and simplify administration (Title II). Title II establishes data security and privacy standards for the transmission, storage, and disclosure of individually identifiable health information, termed protected health information (PHI). HIPAA regulations apply to any "covered entity," which includes health plans, health care clearinghouses, and any health care provider who uses or transmits electronic personally identifiable health information.

HIPAA Privacy Rule

The Privacy Rule establishes requirements and procedures that covered entities and their business associates must meet when storing or transmitting any protected health information (PHI). The rule restricts when and how an individual's protected health information may be used or disclosed. An individual's PHI may only be disclosed (a) to the individual whom is the subject of the PHI (or their authorized agent), (b) to the U.S. Department of Health and Human Services (HHS) as part of an audit or review, (c) as has been otherwise authorized in writing by the individual whom is the subject of the PHI, (d) as part of a covered entity's treatment, payment, and health care operations activities, or (e) other specific circumstances as detailed in the Privacy Rule. Non-compliance with the privacy rule carries civil and criminal penalties. The deadline for compliance with the Privacy Rule is April 14th, 2003.

HIPAA Security Rule

The Security Rule defines standards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). Specifically, HIPAA § 164.306 requires that organizations:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
4. Ensure compliance by its workforce.

More specific requirements are defined to meet the above objectives, including Administrative Safeguards, Physical Safeguards, Technical Safeguards, Organizational Requirements, and Documentation Requirements. Covered entities are given the flexibility to implement the requirements in reasonable and appropriate ways that best fit within that organization that also mitigate the potential risks to ePHI. Organizations are required to perform risk analysis, maintain documentation of its implementation of the Security Rule, and monitor and audit the effectiveness of its controls. The deadline for compliance with the Security Rule is April 21st, 2005.

A key part of the administrative safeguards (HIPAA § 164.308) is the written contingency plan, which requires that organizations have a reasonable plan for ensuring the integrity and availability of ePHI in the event of an emergency or disaster. This plan must provide details on the mechanisms used for data backup and disaster recovery and how these mechanisms comply with the Security Rule.

How Sentinel+ Helps Organizations Comply with HIPAA

Sentinel+'s secure data protection services help partners and their customers meet HIPAA regulations. HIPAA's contingency plan requirement specifies that organizations must implement a data backup and disaster recovery plan that protects electronic protected health information (ePHI) while mitigating risks to the disclosure of ePHI. Sentinel+ can be used as a central part of this plan to automatically and cost-effectively protect ePHI data and provide fast data recovery, while also meeting HIPAA's data privacy, confidentiality, integrity, and availability requirements.

Requirement: Protect Data Privacy and Confidentiality of ePHI

- All data is encrypted before being transmitted in any way, and is only stored or transmitted by Sentinel+ in its encrypted form.
- The encryption key (pass phrase) is only known to the covered entity and/or the Sentinel+ partner. Sentinel+ will never ask for, receive, or record the encryption key or pass phrase. This ensures that the data received and stored by Sentinel+ cannot be decrypted, preventing disclosure of ePHI.
- The data is encrypted using the AES-256-bit algorithm, which has been approved by the NSA for encrypting TOP SECRET data.
- All data transmissions are encrypted with 128-bit AES using the standard TLS/SSL protocol. The identity of the receiving party (the Sentinel+ data center) is authenticated using the public key of Sentinel+'s private certificate authority.
- All access to Sentinel+ accounts and their stored data are protected through password authentication. Passwords are only known to the customer and/or the Sentinel+ partner.
- All access to the account is recorded in an audit log. All actions that modify an account (uploading or destroying data) are recorded in the audit log.

Requirement: Protect Data Integrity of ePHI

Sentinel+ is uniquely positioned to help companies comply with the data integrity requirement within their HIPAA contingency plans. Additional details of the below provisions are in our data integrity whitepaper.

- Each data block is digitally signed with an HMAC [HMAC-SHA-256] to allow for automatic validation during restores that the data has not been altered or tampered with.
- Sentinel+ uses checksums on the data as it moves across the network, inside the Sentinel+ servers and server software, through the operating system and device drivers, and all the way down to the final storage medium to ensure that the data remains perfectly intact and did not change while being transmitted from the client computer to the storage devices in our data centers.
- Sentinel+ uses high levels of data redundancy with redundant checksums to ensure that any silent data corruption is automatically detected and repaired using the redundant information.
- The integrity of the data is checked when files change as well as through scheduled checks.

Requirement: Protect ePHI from Reasonably Anticipated Threats/Hazards

- Physical Security: Our data centers are protected by 24/7/365 guards and CC surveillance, card-key access, biometrics, partitioned floor space with access control, and secure locking cabinets.
- Network Security: We use multi-level firewalls and intrusion detection systems to filter/analyze all traffic. Access controls uniquely identify users and log all access.
- Sentinel+'s infrastructure is fully fault tolerant. Measures include backup generators and UPS systems, redundant power feeds, fire detection and suppression, multi-homed connectivity, environmental monitoring, redundant storage controllers and connections, redundant server power supplies, stocked spare-parts, and 2-hour hardware replacement service contracts.