HIPAA Compliance Data Sheet

DATA REGULATORY COMPLIANCE

The importance of always available and accurate health care data is integral to delivering quality care. The ability to recover data at a desired point-in-time can make the difference in a health care delivery system.

In 2003, the HIPAA Privacy Rule set national standards for the protection of health information, as applied to three types of covered entities: health plans, health care clearinghouses and health care providers who conduct transactions electronically. Entities must maintain standards to ensure data integrity, availability and the security of individually identifiable health information.

HIPAA Data Compliance Requirements

The data management portion of HIPAA is focused on the secure storage and transmission of Protected Health Information (PHI) over computer networks. PHI includes all individually identifiable health records in any form or media including subsets of health information such as demographics. HIPAA defines who is authorized to access this information and requires the establishment and maintenance of appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiality, and availability of the information.

Healthcare organizations are required to individually assess their security and privacy requirements and take measures to implement electronic data protection for data in transit and storage.

HIPAA REQUIREMENT	ABS COMPLIANCE STANDARDS
Electronic protected health information (ePHI) must be secured against potential threats or hazards.	Data is securely stored in two geographically diverse datacenters. Redundant fail-safe systems protect the data in every step of the backup and storage process.
Access to ePHI must be protected against any reasonably anticipated uses or disclosures that are not permitted or required by the Privacy Rule.	Data is encrypted with 256-bit AES encryption technology. Access is restricted by password authentication.
Maintenance of record of access authorizations.	Reporting provides a clear audit trail with user access date and time-stamp detail.
If the data is processed through a third party (ABS), entities are required to enter into a chain of trust agreement.	ABS and the Partner enter into a Service Agreement. This outlines that the parties agree to electronic exchange of Customers data and that ABS is provisioned to protect and maintain the integrity of the transmitted data.

ABS
ADVANCED BACKUP SOLUTIONS