DATATRUST
SOLUTIONS

How Secure Archive Manager
Meets HIPAA Requirements

The Secure Archive Manager data management application enables customers to archive information and meet regulatory compliance requirements. This document covers how the Secure Archive Manager can help customers comply with the regulations in the Health Insurance Portability and Accountability Act (HIPAA).

The Department of Health and Human Services administers HIPAA. The Act is composed of two rules, the first covers privacy and second covers security. The privacy rule has many parts that relate to the handling of patient information and are covered below. The privacy rule took effect on April 14, 2004. The security rule went into effect on April 21, 2005 and has significant implications in the managing and storing of computerized information. Beginning in 2006, enforcement of HIPAA rules has led to civil penalties and fines for institutions not complying. The increasing number of audits and threats of audits has led to a new urgency in understanding what is required of professionals in information technology to comply with the law.

DataTrust Solutions developed the Secure Archive Manager to specifically meet the unique needs of managing records and data for customers in regulated industries. Secure Archive Manger is a hardware independent data management application that provides immutability, retention, legal hold, and data disposition and encryption functionality. Secure Archive Manager works with a wide variety of direct attached disk, network storage and cloud options enabling them with security and compliance required features. This document addresses how Secure Archive Manager helps customers comply with HIPAA requirements and rules.

Information Storage Requirement for HIPAA

Protected Health Information (PHI) is the term describing healthcare data that is subject to the privacy and security rules of HIPAA. There are many areas of handling data that have proscriptive rules, but the handling of PHI in computerized operations has had the most focus from an enforcement standpoint. The elements of privacy and security in the area of technical safeguards that must be addressed and how Secure Archive Manager meets the requirements are noted in the following table:

Action	Secure Archive Manager
Control of access to information	SAM requires that authentication be established to allow authorized access to information managed by SAM. All users must establish indemnity and provide the correct password to access and information on SAM. To access administrative functions a user must be previously assigned the special role of Administrator by the primary System Administrator.
Audit trail of access	SAM maintains an audit trail log of every action taken on a file. The audit trail includes information about the ingestion, every subsequent access, file locations, and any Policies such as retention period, legal hold or data disposition. The audit trail log provides a complete chain-of-custody for the PHI over its lifecycle.
Data protection – availability	A Policy can be set for an archive to create a minimum of two copies to be automatically made during the ingest process for PHI data. The Administrator can set the Copy Policies to make additional copies and data written to alternative locations physical locations.

Data protection – retention	The Administrator can create independent archives within SAM for data segregation. Policy settings for each archive can be enabled with WORM or retention settings. Ingested files will be retained indefinitely if a Write Once, Read Many (WORM) Policy is set for the archive. Ingested files will be retained in the archive until the retention period has expired for files under a Retention Policy. A legal Hold Policy can be used to extend the retention of files in an archive for a definable period of time beyond the retention period. Folders within an archive may be configured with different retention settings.
Data integrity – protection from alteration or destruction	SAM stores PHI in archives configured with WORM or Retention Policies on storage media or to cloud storage. PHI data under WORM or Retention policies is protected from alteration or deletion until the retention period has expired. SAM uses a content based cryptographic hash algorithm is performed on the data to produce a unique digital fingerprint to verify that no data has been changed during any transmission or storage operation. Additionally, SAM provides encryption (AES-256 algorithm) to further protect data. Data can also be converted to objects only identifiable and accessible by SAM for further data protection.
Data protection – encryption	Data stored on non-directly controllable storage such as network storage or in cloud storage must be encrypted to be considered protected. SAM uses an AES- 256 algorithm and individually encrypts each file with a different key. SAM manages all of the encryption keys ensuring security and eliminating the need to manage them separately.

Summary

The enforcement of HIPAA commenced in 2006 and is being used as a means to ensure that organizations such as hospitals, clinics, doctor's offices, etc., are complying with Department of Health and Human Services rules and laws. Not complying with HIPAA has led to significant civil and criminal penalties.

Secure Archive Manager provides an easy and efficient means to meet the legal requirements of HIPAA, while providing significant economic benefits for archiving of data. Most PHI data subject to HIPAA rules will outlive the storage the data is written on and the organization is responsible for adhering to the privacy and security rules during the transitioning of the data from one storage system to another as well as on the new storage area. Secure Archive Manager operates independent of any storage system enables IT to manage data over its legal life cycle.