

Compliance Requirements for Email Archiving

HEALTHCARE RETENTION REQUIREMENTS

HIPAA

- Email messages must be retained for six years & two years after a patient's death.
- Retained content must be stored in a robust data center that provides minimum guaranteed uptime and very high security.

Medicare

All medical records must be retained for five years.

Legal Discovery

Email retention policies must consider:

- The lack of a policy is not considered a policy
- Production of records from back up tapes is a wasteful proposition
- Quick response times during discovery for what can be produced and what cannot

SONIAN: SECURE. RELIABLE. SCALABLE.

Robust

Sonian uses cloud-compute infrastructure for scalability and reliability. Sonian's unique and differentiated cloud-compute software stack harnesses on-demand CPU and geographically dispersed storage to power archival functions for data ingestion, indexing, search, eDiscovery and export. The Sonian system uses map-reduce style parallel processing to search very large data sets in sub-second response times. Parallel processing is only possible with cloud-compute CPU, taking advantage of the ability to scale up in real-time so that every customer search experience is quick and there is no waiting for jobs to complete.

Unlimited Storage

Storage capacity automatically increases on a per customer basis, at no cost. Regardless of how much email you add, you will never run out of storage, or be charged additional fees. Cloud-based storage allows for continuous uninterrupted data growth without the cost and capacity issues that plague traditional storage architectures.

Ease of Use

With no hardware to buy or software to install, you can be up and running immediately. The simple and intuitive web-based interface allows for easy archive set up and our support team provides training for you and your staff. Rapid search and retrieval is possible by individuals in a personal archive, or across the whole archive by authorized users such as lawyers or compliance officers —without burdening your IT staff.

Security and Privacy

Sonian data security exists at three levels: physical infrastructure, data encryption, and the application layer. Data is secured in transit, and at rest. Our data storage meets rigorous PCI DSS standards (Payment Card Industry Data Security Standard) and the guidelines set forth by the Cloud Security Alliance. All data is secured via industry standard encryption (Defense Department AES and SSL), with no shared encryption keys across customers. There is never any co-mingling of archived data between customers. At the application layer, Sonian uses Secure Socket Layers (SSL) to encrypt all communication between the web browser and the data center, and a processing pipeline that ensures performance and data privacy between customer accounts.



Sonian is the trusted cloud-powered universal data management company, which delivers archiving/storage, eDiscovery and compliance services. Global organizations rely on Sonian for its affordability, security, ease of deployment and use. Founded in 2006, Sonian supports thousands of customers on all major enterprise collaboration solutions including Exchange, Notes, GroupWise, Zimbra and others; and enjoys strategic partnerships with industry leaders Amazon Web Services, Rackspace, Axway and IBM.

Sonian, Inc.
100 Crescent Road
Needham, MA 02494
617.958.4000
www.sonian.com

Compliance Requirements for Email Archiving

Budget and ROI

A fixed cost per user via a simple monthly subscription makes planning easy. Migrating your data into the cloud allows you to reduce storage and maintenance costs, reallocate or eliminate on-premise or hosted servers, avoid compliance fines and fees associated with data loss, and reduce the costs associated with

eDiscovery and analysis by leveraging Sonian's easy to use UI for early case assessment.

Compliant

36 CFR 1220.34, 36 CFR 1220.38, U.S. Department of Defense Directive 5015.2, NPG 1441.1C, FOIA, Legal Discovery