



# Data Management Policy

Marketware, Inc. has procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI) stored in conjunction with Marketware, Inc. Add-ons and for PaaS Customers utilizing our Backup Service. The policy and procedures will assure that complete, accurate, retrievable, and tested backups are available for all systems used by Marketware, Inc.

Data backup is an important part of the day-to-day operations of Marketware, Inc. To protect the confidentiality, integrity, and availability of ePHI, both for Marketware, Inc. and Marketware, Inc. Customers, complete backups are done daily to assure that data remains available when it needed and in case of disaster.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment.

## Applicable Standards from the HITRUST Common Security Framework

- 01.v - Information Access Restriction

## Applicable Standards from the HIPAA Security Rule

- 164.308(a)(7)(ii)(A) - Data Backup Plan
- 164.310(d)(2)(iii) - Accountability
- 164.310(d)(2)(iv) - Data Backup and Storage

## Backup Policy and Procedures

- Perform daily snapshot backups of all systems that process, store, or transmit ePHI for Marketware, Inc. Customers.
- Marketware, Inc. Ops Team, lead by VP of Business Intelligence, is designated to be in charge of backups.
- Dev Ops Team members are trained and assigned to complete backups and manage the backup media.
- Amazon S3 Storage is used to backup Server and Database snapshots.
- Backups are performed nightly and backups are retained in S3 for 7 days for immediate retrieval, then archived via Amazon Glacier.
- Securely encrypt stored backups in a manner that protects them from loss or environmental damage.
- Test backups and document that files have been completely and accurately restored from the backup media.