COMPLIANCE

Health Information Portability and Accountability Act (HIPAA) Compliance with Rocket® Mainstar® Backup and Recovery Manager Suite

The Health Information Portability and Accountability Act (HIPAA) requires organizations to safeguard patients' protected health information (PHI), restricting and monitoring access to any systems that house it. HIPAA includes a privacy rule concerned with appropriateness and disclosures of collected, stored, or distributed information, and patients' ability to opt out of certain information usages. The HIPAA security rule includes numerous control requirements intended to protect the confidentiality, availability, and integrity of PHI.

The HIPAA security rule is available at 45 C.F.R. 164.302-316, and implementation guidance is provided in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66.

Rocket® Mainstar® Backup and Recovery Manager Suite (BRMS) centralizes your backup and recovery management processes for an IBM® z/OS® environment. With BRMS, you can be sure that your PHI is secure and available. Relevant HIPAA requirements and the associated capabilities BRMS offers are listed below.

HIPAA REQUIREMENTS	BRMS CAPABILITIES
Contingency Plan:164.308(a)(7) Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	BRMS performs analysis to identify all critical datasets and determine whether they're included in your backup processes, or whether they're omitted or outdated. BRMS provides a centralized management interface to configure, monitor, and report on the various predefined backup jobs executed by all your backup software for the entire IBM z/OS environment. Interfaces with your backup software let BRMS generate backup jobs to cover any missing datasets. Reporting functionality shows the status of each dataset and each backup or restoration task, to ensure successful completion. BRMS automatically generates jobs to restore datasets that can be used for periodic testing requirements. Restoration jobs are customized to include the datasets specifically required to restore a given application.
Access Control: 164.312(a)(1) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	BRMS leverages your TSO credentials and all associated authentication mechanisms. There is no need to maintain a separate user account list in BRMS. IBM Security Authorization Facility (SAF) provides standard access controls over data based on the TSO login. BRMS functions validate that the user has SAF rights and cannot bypass mainframe access restrictions. BRMS enhances the capabilities of native ABARS facilities to ensure that restored files cannot have modified security permissions, protecting the confidentiality within the restored files.

HIPAA REQUIREMENTS	BRMS CAPABILITIES
Audit Controls: 164.312(b) Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	All relevant changes to user accounts, roles, and assigned permissions through the SAF are fully logged through the IBM System Management Facility (SMF). Reporting and alerting on such actions can be configured through the mainframe functions. All actions performed through BRMS against backup jobs and datasets are traceable to individual users executing the function. Detailed logging is available through the IBM Resource Access Control Facility (RACF).
Integrity: 164.312(c)(1) Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	BRMS Manager offers monitoring of backup job status that enables you to identify errors that could result in compromised data integrity of your backup volumes.
Person or Entity Authentication: 164.312(d) IImplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	BRMS leverages the logged-in user credentials of the native IBM TSO function. TSO credentials, and all authentication mechanisms tied to that login, are inherited by BRMS.
Documentation: 164.316(b)(1) (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment. (ii) Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Backup collection logs and reports are retained with BRMS to maintain historical evidence for auditors and examiners.

Rocket®

rocketsoftware.com

info@rocketsoftware.com

US: 1 877 577 4323
EMEA: 0800 520 0439
APAC: 1800 823 405

twitter.com/rocket

www.linkedin.com/company/rocket-software

www.facebook.com/RocketSoftwareInc

blog.rocketsoftware.com