COMPLIANCE

# Health Information Portability and Accountability Act (HIPAA) Compliance with Rocket® Mainstar® Catalog RecoveryPlus

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® Catalog RecoveryPlus (CR+) does not directly store or process PHI; it ensures that the metadata used to manage data stored in an IBM® z/OS® environment is properly backed up and recoverable. However, HIPAA requires contingency planning, data availability, and data integrity controls, and CR+ can play an integral part in these functions. Relevant HIPAA requirements and the capabilities Mainstar CR+ offers to address them are listed below.

| HIPAA REQUIREMENTS | CR+ CAPABILITIES |
| --- | --- |
| Contingency Plan:164.308(a)(7)<br>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. | The health of your ICF catalogs is crucial to ensuring the availability of your mainframe data. CR+ monitors your ICF catalogs enterprise-wide to verify that they're appropriately backed up and recoverable.<br><br>CR+ allows routine maintenance of ICF catalogs during operation without outages, reducing downtime and supporting 24x7 high-availability environments.<br><br>CR+ can analyze your disaster recovery site's ICF catalogs and synchronize them with your production data. |
| Access Control: 164.312(a)(1)<br>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). | Detailed, customizable permissions can be configured for each user to support the rule of least privilege and segregation of duties. Permissions can apply to both the data being accessed and the function being performed.<br><br>IBM Security Authorization Facility (SAF) provides the standard access controls over data. CR+ defines new profiles that add function-based access controls.<br><br>CR+ supports role-based permissions management for consistent application of user rights, as well as individual rights assignments for specific needs.<br><br>Specific reports are available from CR+ showing the function-level permissions granted through its access profiles. You can use these to validate the appropriateness of assigned rights. |

| HIPAA REQUIREMENTS | CR+ CAPABILITIES |
| --- | --- |
| Audit Controls: 164.312(b)<br>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 Security Authorization Facility (SAF) are fully logged through the System Management Facility (SMF). Reporting and alerting on such actions can be configured through the mainframe functions. |
| Integrity: 164.312(c)(1)<br>Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | CR+ performs diagnostics of relationships between data sets and ICF catalogs to identify integrity problems that could impair your data recovery capabilities, and automatically generate fix commands. |
| Person or Entity Authentication: 164.312(d)<br>IImplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | CR+ leverages the logged-in user credentials of the native IBM TSO function. TSO credentials, and all authentication mechanisms tied to that login, are inherited CR+. |



Rocket

rocketsoftware.com
info@rocketsoftware.com
US: 1 855 577 4323
EMEA: 0800 520 0439
APAC: 612 9412 5400
twitter.com/rocket
www.linkedin.com/company/rocket-software
www.facebook.com/RocketSoftwareInc
blog.rocketsoftware.com