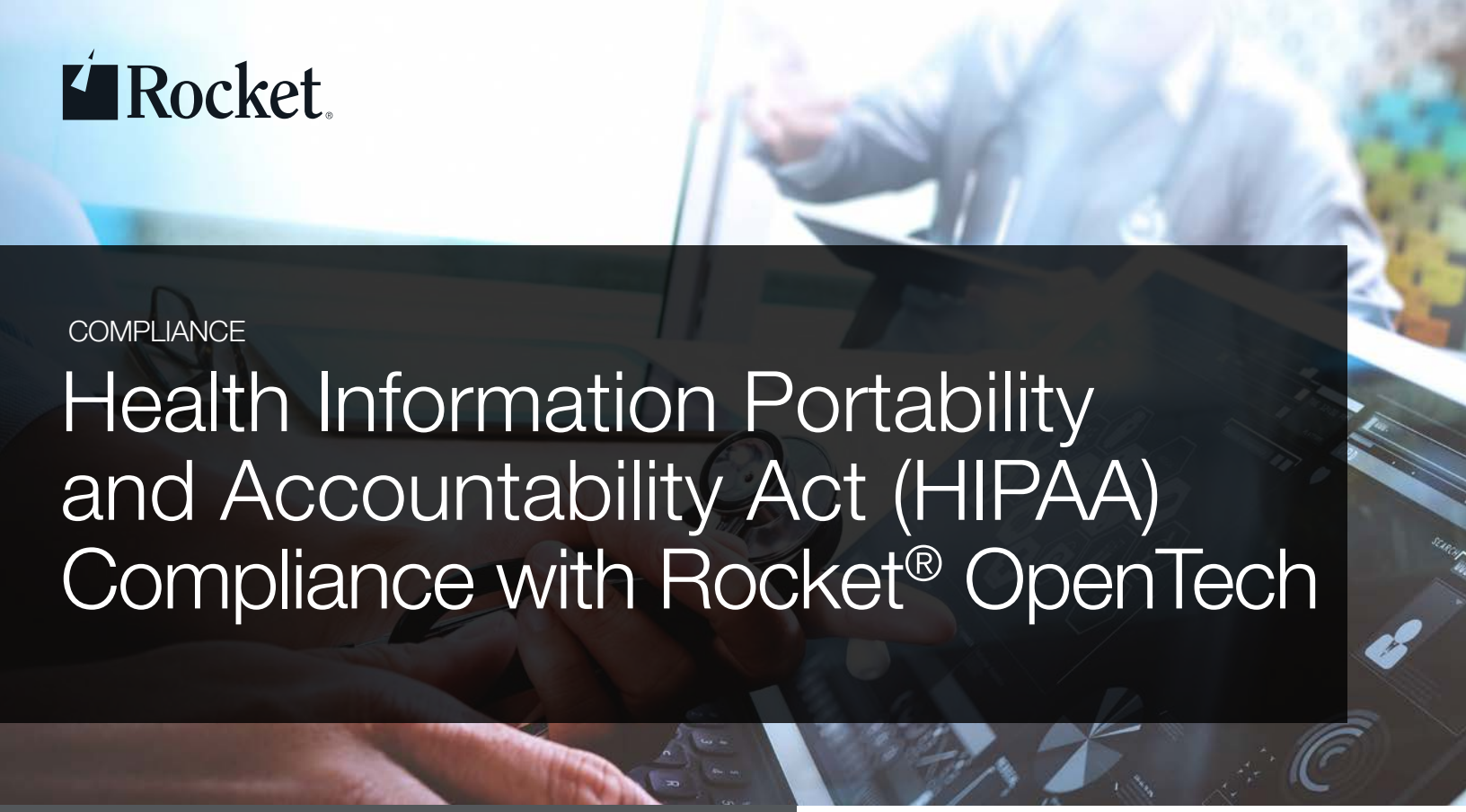

COMPLIANCE

# Health Information Portability and Accountability Act (HIPAA) Compliance with Rocket® OpenTech

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® OpenTech products provide you with all the tools you need to implement a strong backup management program and availability controls for your entire IBM®z/OS® environment—from executing backup and migration jobs, to monitoring job statuses, to simulating restoration events, and more. The OpenTech portfolio includes Rocket DR/Xpert, Rocket DASD Backup Supervisor, Rocket Tape/Copy, Rocket Virtual Data Recovery, and Rocket CopyExport Manager.

Relevant HIPAA requirements, and the capabilities OpenTech products offer to address them, are listed below.


| HIPAA REQUIREMENTS | OPENTECH 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. | DR/Xpert helps analyze all your backup jobs and datasets to automatically identify those that are critical, especially any that could contain PHI. This reduces your risk of unknowingly omitting PHI from your backup program. The system also continuously monitors for changes to these critical data volumes.<br><br>DR/Xpert provides monitoring and reporting to ensure that all critical datasets have backed-up or mirrored datasets available, and that the backup data is current. It also provides facilities in the event of a disaster recovery incident for managing restoration tasks, and allows prioritization for PHI recovery.<br><br>DR/Xpert centrally manages your backup utilities (such as Tape/Copy) to automatically generate backup jobs, as well as restoration jobs for when they're needed, and integrates them with your job scheduling.<br><br>DASD Backup Supervisor continuously monitors your storage for new or modified volumes, and maintains backup jobs to ensure that they are reliably performed. It also generates automated recovery jobs associated with its backup tapes to be stored alongside the data for quick, simple, and efficient restoration.<br><br>Tape/Copy executes the backup process from tapes to other media, and builds in error reporting and recovery features to ensure all your data volumes remain intact.<br><br>CopyExport Manager enhances the capabilities of the native copy export process by adding automatic error detection and reporting for archival of your critical data sets from virtual tape libraries to physical tapes. |

| HIPAA REQUIREMENTS | OPENTECH CAPABILITIES |
|---|---|
| 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). | OpenTech products leverage the logged-in user credentials of the native IBM TSO function. TSO credentials, and all authentication mechanisms tied to that login, are inherited by OpenTech products.<br><br>IBM Security Authorization Facility (SAF) provides standard access controls over data based on the TSO login. OpenTech product functions validate that the user has SAF rights and cannot bypass mainframe access restrictions.<br><br>While certain features such as the Tape/Copy tape browse function allow access to data within backup volumes, this access is still restricted by the SAF permissions for the logged-in user. |
| 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 SAF are fully logged through the IBM System Management Facility (SMF). Reporting and alerting on such actions can be configured through the mainframe functions.<br><br>All actions performed through OpenTech products 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)<br>Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | Tape/Copy integrates data validation controls to detect any errors in the conversion process, preventing any data integrity issues from being transferred to the new media.<br><br>CopyExport Manager enhances the capabilities of the native copy export process by adding automatic error detection and reporting for archival of your critical data sets from virtual tape libraries to physical tapes. |
| Person or Entity Authentication: 164.312(d)<br>Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | OpenTech products leverage the logged-in user credentials of the native IBM TSO function. TSO credentials and all authentication mechanisms tied to that login are inherited by OpenTech products. |

| HIPAA REQUIREMENTS | OPENTECH CAPABILITIES |
| --- | --- |
| Documentation: 164.316(b)(1)<br>(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.<br><br>(ii) Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. | DR/Xpert provides monitoring and reporting functionality for your entire backup environment. Logs and reports can serve as evidence for auditors or examiners that your backup process is operating effectively. |



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