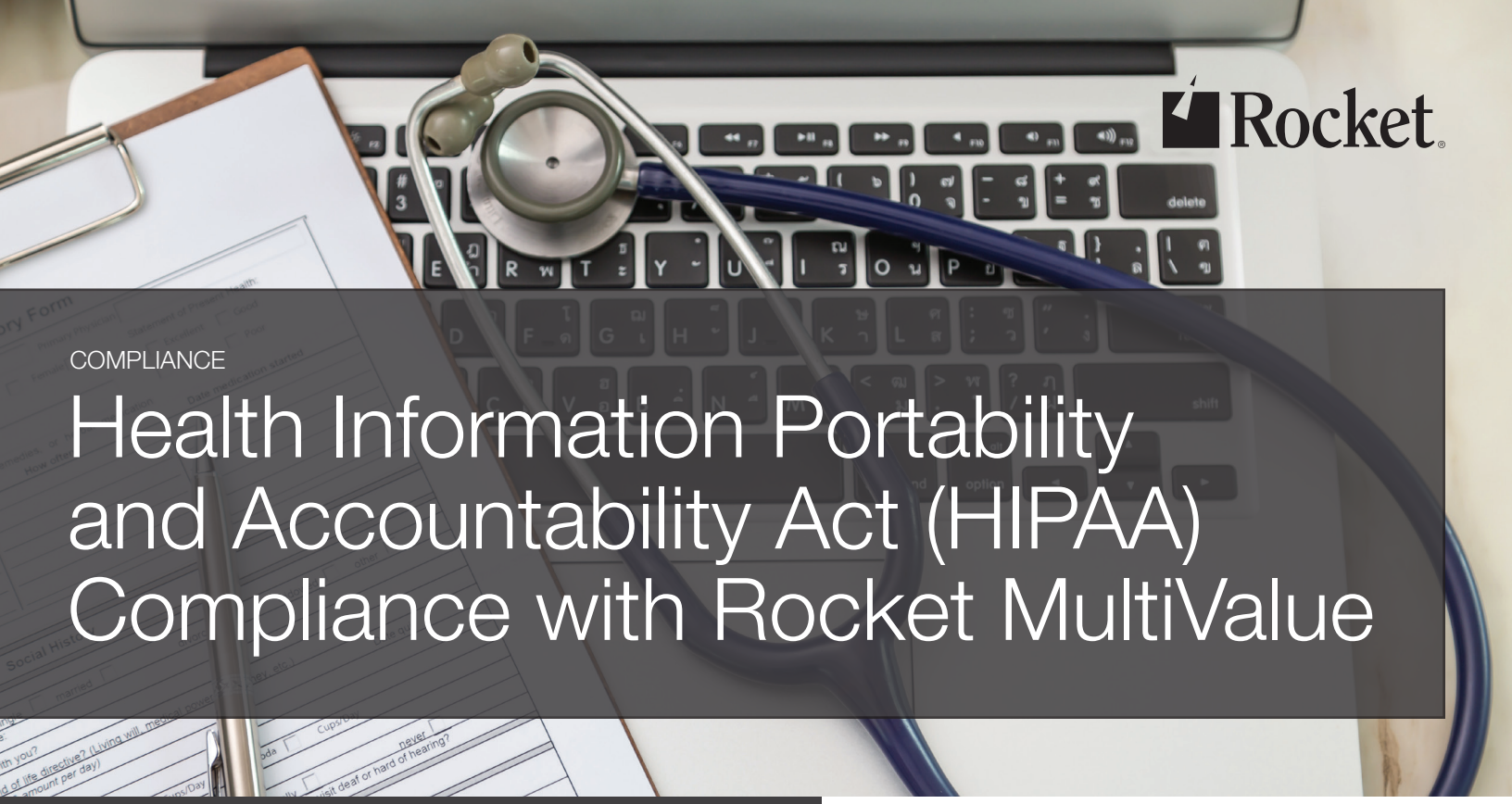

COMPLIANCE

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

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 that concerns appropriateness and disclosures of collected, stored, or distributed information, and patients' ability to opt out of certain information usages. The HIPAA security rule includes several 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.

The Rocket® MultiValue Application Platform (Rocket MV), which includes Rocket UniData, Rocket UniVerse, and Rocket D3, gives you the flexibility to implement secure technical and procedural control operations into your databases that house ePHI. This includes HIPAA's user access and data integrity requirements, as well as the requirement for logging and monitoring access to ePHI that can often be difficult to address. Relevant HIPAA requirements and the capabilities Rocket MV offers are listed below.

| HIPAA Requirements | Rocket MV Capabilities |
| --- | --- |
| Workforce Security: 164.308(a)(3)<br>Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | Rocket MV implements both database-level access controls and user-level, role-based access controls. Retrieval locks and update locks (read and write access) can be configured granularly to support your confidentiality requirements and protect sensitive information. Information access and disclosure is limited to authorized users.<br><br>User authentication is performed by the operating system and passed to the database. Rocket MV supports username and password sets from Microsoft and UNIX systems, as well as token-based single sign-on (SSO). |
| Information Access Management: 164.308(a)(4)<br>Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. | All administration of user access and database security features is performed through a database management console, with access restricted to designated administrative users.<br><br>Audit logs can provide a secure record of any access or updates to user access rights, whether authorized or unauthorized. |
| 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. | Recoverable File System (RFS) helps maintain the physical integrity of data at rest and ensure recovery from hardware failures.<br><br>Delayed Standby Replication lets you protect a subscriber from malicious damage caused by a compromise to the publisher. Real-time replication may introduce the same damage from the publisher to the subscriber, exposing you to potential data loss. Keeping the subscriber a defined interval behind the publisher (such as 6 hours) protects the business and helps address ‘Clear record’ events. |
| 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). | Rocket MV implements both database-level access controls and user-level, role-based access controls. Retrieval locks and update locks (read and write access) can be configured granularly to support your confidentiality requirements and protect sensitive information. Information access and disclosure is limited to authorized users.<br><br>All administration of user access and database security features is performed through a database management console, with access restricted to designated administrative users.<br><br>Audit logs can provide a secure record of any modification of user access rights, whether authorized or unauthorized.<br><br>Audit logging configuration is stored in an encrypted file that can be password-protected and is only modifiable by authorized users. |

| HIPAA Requirements | Rocket MV 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. | Detailed audit logging and reporting capabilities can help you determine exactly which records were accessed, when, and by whom. This will support a regular control operation to monitor access to ePHI or an investigation into suspected unauthorized activity.<br><br>Audit logging configuration is stored in an encrypted file that can be password-protected and is only modifiable by authorized users. |
| Integrity: 164.312(c)(1)<br>Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | Recoverable File System (RFS) helps maintain physical integrity of data at rest and ensure recovery from hardware failures.<br><br>OpenSSL-based Automatic Data Encryption protects data in transit, in use, and at rest. This encryption also protects the integrity of the data being sent and received, to prevent inaccuracies. Parties can be certain they are talking to the intended party, and that data has not been corrupted or maliciously altered during transmission.<br><br>Data integrity is protected from malicious or unauthorized alteration through role-based, Active Directory-integrated access rights management. Rocket MV can enforce granular write/update access for individual users. |
| 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. | User authentication is performed by the operating system and passed to the database. Rocket MV supports username and password sets from Microsoft and UNIX systems, as well as token-based single sign-on (SSO). |
| Person Transmission Security: 164.312(e)(1)<br>Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | OpenSSL-based Automatic Data Encryption protects data in transit, in use, and at rest. This encryption also protects the integrity of the data being sent and received, to prevent inaccuracies. Parties can be certain they are talking to the intended party, and that data has not been corrupted or maliciously altered during transmission. |

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