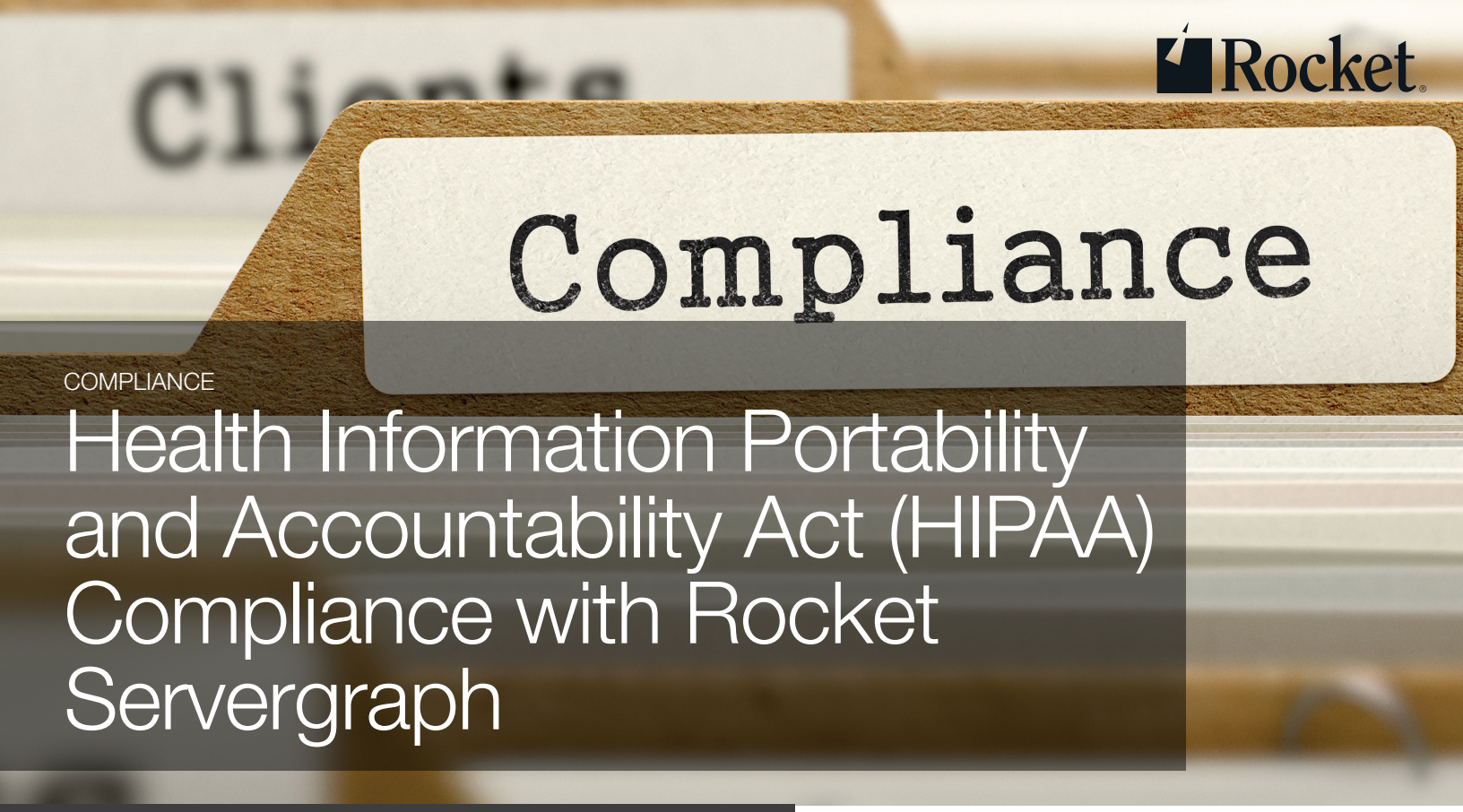

COMPLIANCE

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

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 the ability of patients to opt-out of certain information usages. The HIPAA security rule features a number of 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.

In typical implementations, your PHI would never be stored directly within Rocket® Servergraph. The Servergraph solution collects only metadata surrounding your backup process, not the content of the backed up data. However, Servergraph can support the contingency planning, data availability, and data integrity controls that HIPAA requires. The relevant HIPAA requirements and capabilities that Servergraph offers are listed on the following pages.

HIPAA REQUIREMENTS	ROCKET SERVERGRAPH 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 PHI.	Servergraph collects information from backup software, hardware, and processes in your environment to document that data backups are operating in accordance with your organizational policies. Traps, reports, and alerts are customizable to capture relevant information for all of your backup control requirements. Reports and alerts can be automatically distributed to any individuals, supporting segregation of duties and facilitating review and monitoring processes. Backup collection logs and reports are retained within Servergraph for a fully configurable duration to maintain historical evidence. The Server Monitor feature shows real-time statistics and alerts for backup systems such as storage utilization and disk capacity.
Facility Access Controls: 164.310(a)(1) Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Systems are installed on premise, and the organization can implement physical and environmental controls as with all other computing equipment.
Access Control: 164.312(a)(1) Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	Servergraph is agentless and requires only a read-only service account to operate, preventing unintentional or unauthorised modification of network systems and data. Servergraph supports unique user IDs for all individuals accessing the system, and uses LDAP integration with Active Directory credentials. System administration is performed through the separate administration client, with access restricted to designated administrative users. Detailed, customisable permissions can be configured for each user to support the rule of least privilege and segregation of duties.
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 PHI.	Systems logs are available to record all data collection activities performed by Servergraph over your backup systems.
Integrity: 164.312(c)(1) Implement policies and procedures to protect electronic PHI from improper alteration or destruction.	Servergraph is agentless and requires only a read-only service account to operate, preventing unintentional or unauthorized modification of network systems and data.
Person or Entity Authentication: 164.312(d) Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.	Passwords are required for all users attempting to log into the system. Local credentials are stored in encrypted hash format. Servergraph offers LDAP integration with Active Directory credentials, inheriting your organization's network-level authentication requirements.
Person Transmission Security: 164.312(e)(1) Implement technical security measures to guard against unauthorized access to electronic PHI that is transmitted over an electronic communications network.	PHI should not be included in the metadata collected by Servergraph. However, Servergraph supports encrypted Secure Shell (SSH) sessions for all data collection activities. Users access the web-based Servergraph application using encrypted HTTPS sessions.

HIPAA REQUIREMENTS	ROCKET SERVERGRAPH CAPABILITIES
Documentation: 164.316(b)(1) (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form. (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. (iii) Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Servergraph collects information from backup software, hardware, and processes in your environment to demonstrate that data backups are operating in accordance with your organizational policies. Reports and alerts can be automatically distributed to any individuals, supporting segregation of duties and facilitating review and monitoring processes.
Documentation Specifications: 164.316(b)(2) (i) Time limit: Retain the documentation required by paragraph (b)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later. (ii) Availability: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. (iii) Updates: Review documentation periodically and update as needed in response to environmental or operational changes affecting the security of the electronic PHI.	Backup collection logs and reports are retained within Servergraph for a fully configurable duration to maintain historical evidence.

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