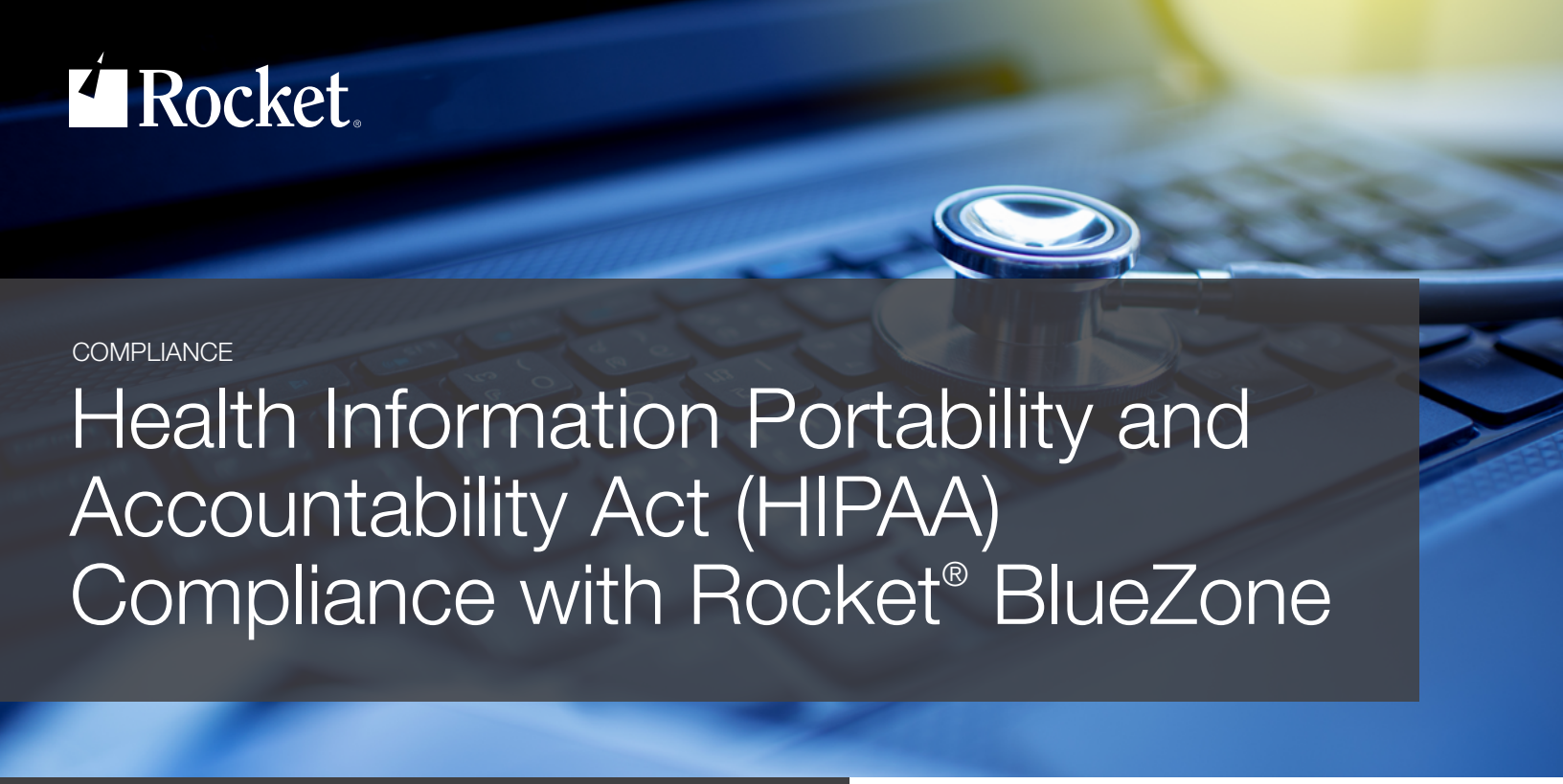
Rocket



COMPLIANCE

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

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, which concerns appropriateness and disclosures of information that is collected, stored, or distributed and the ability for a patient to opt-out of certain information usages. The HIPAA security rule includes 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.

Rocket BlueZone terminal emulation solutions do not store any data directly and leverages your host system environment for access controls to protect the confidentiality of PHI. You don't need to manage additional user credentials and authorization processes for BlueZone to maintain effective logical security. BlueZone also provides enhanced logging and remote access security capabilities, as well as and strong encryption to protect all data throughout its usage. Relevant HIPAA requirements and the capabilities BlueZone offers are listed below.

HIPAA REQUIREMENTS	BLUEZONE CAPABILITIES
Workforce Security: 164.308(a)(3) 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.	BlueZone provides communication between clients and backend host systems by utilizing the user access permissions inherent to the backend host system environment. BlueZone cannot provide any capability for data access that is not already specifically authorized within your host system O/S to the logged in user.
Information Access Management: 164.308(a)(4) 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.	BlueZone leverages your host system credentials and permissions. There is no need to maintain a separate user account list in BlueZone or to separately authorize PHI access.
Security Incident Procedures: 164.308(a)(6) Implement policies and procedures to address security incidents.	In the event of a breach, any BlueZone activity from the affected time period would be evidenced in your host system logs for a forensic investigation. Logging capability is enhanced with BlueZone Web, as you can identify not only which commands were executed against the host system, but also all terminals and users who have connected to your systems, along with the date, time, and source address. This information can be critical to an effective response process.
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.	The distributed nature of BlueZone's architecture allows administrators to connect to the host system environment from anywhere, to anywhere. During a technical incident or disaster scenario, BlueZone can help continue or restore operations and access to PHI. BlueZone clients can specify alternate hosts for instant cutover to disaster recovery facilities.
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).	All user accounts and access permissions are inherited from the host system. BlueZone cannot provide any capability for data access that is not already specifically authorized within your host system O/S to the logged in user. Security Server provides an additional, optional layer of security by acting as a proxy between your host system and clients. Clients must first connect and authenticate to your Security Server using an established user ID, which may be integrated with other Identity Access Management systems including RSA and Active Directory. After authenticating to Security Server, users must then also login to the host system directly, applying the host system-level access permissions.

HIPAA REQUIREMENTS	BLUEZONE 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.	The built-in logging mechanisms inherent to your host system environment record all activities initiated through BlueZone sessions. There is no need to maintain a separate log management function specifically for BlueZone. As a supplemental logging mechanism, Rocket BlueZone Web records a log of all client connections to the web server. This does not record commands issued through the sessions, which would be logged through the built-in host system functionality, but provides an additional layer of security by showing how many users and terminals are connecting, when, and from where.
Integrity: 164.312(c)(1) Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Encryption of data in transit protects the integrity of all such data, preventing technical errors, corruption, or malicious alteration in transit that could impair its accuracy and reliability.
Person or Entity Authentication: 164.312(d) Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Authentication is performed against the host system directly, applying its password requirements and other authentication mechanisms, which may include physical tokens, client-side X.509 certificates, and other multi-factor authentication systems. When using Security Server, a second layer of authentication against the Security Server directly before a user may attempt to authenticate to the host system. Security Server supports integration with RSA SecurID and Active Directory for user credentials and authentication.
Transmission Security: 164.312(e)(1) Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	BlueZone products supports state-of-the-art encryption methods for all communications between clients and the backend host system environment, including the TLS1.2 are SSHv2 protocols with FIPS-compliant encryption algorithms. BlueZone Web applies this level of encryption to both the end user-to-web server session, and the web server-to-host system session. While support for older protocols is available to support legacy systems, this support can be disabled entirely to prevent any potential security vulnerabilities. In environments where the host system cannot support encrypted sessions, the optional Security Server allows for plaintext communications to be isolated within a secure, local network, while applying strong encryption methods to all external connections with clients.

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