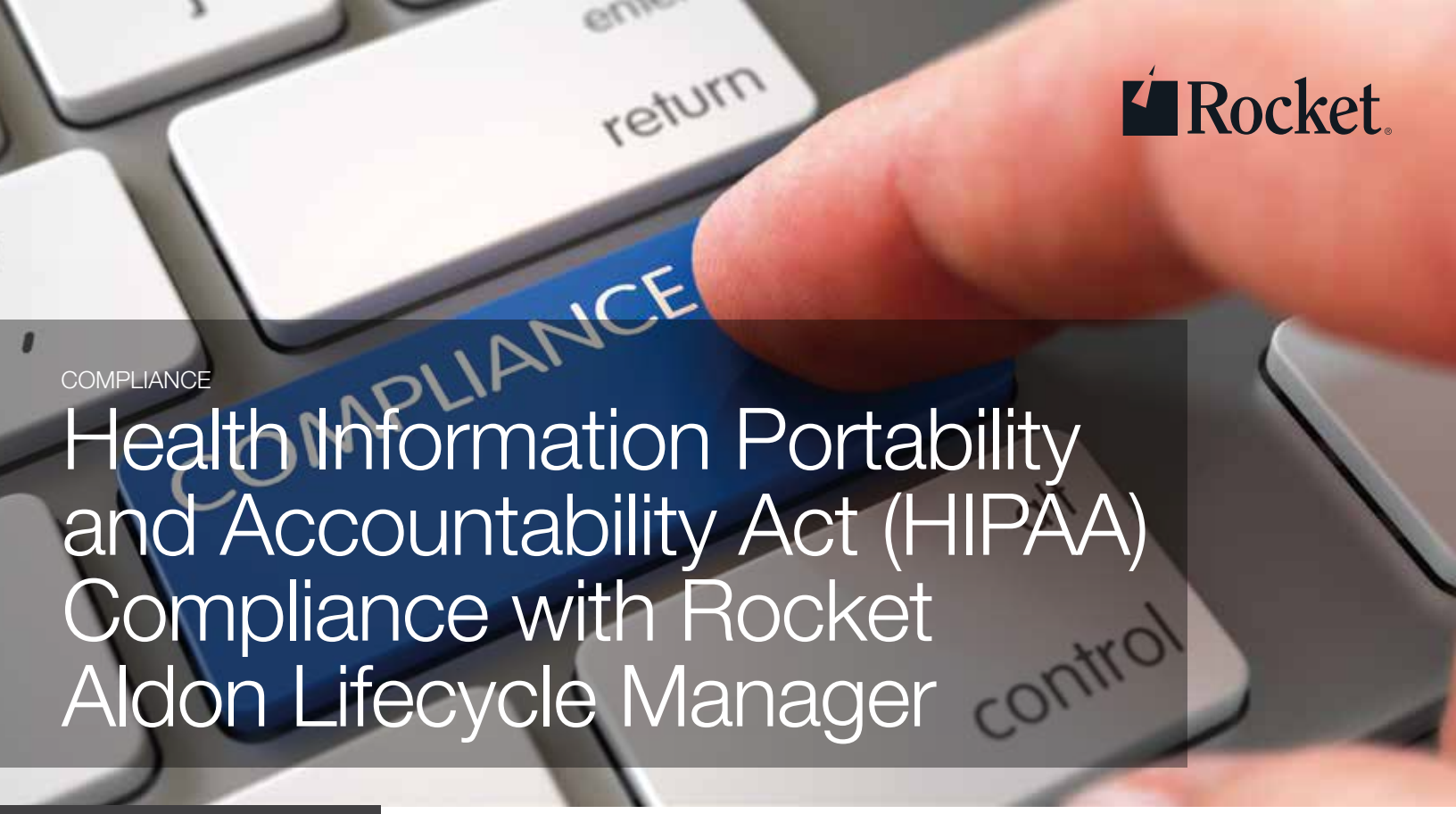


COMPLIANCE

# Health Information Portability and Accountability Act (HIPAA) Compliance with Rocket Aldon Lifecycle Manager

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® Aldon Lifecycle Manager is unlikely to contain any PHI. While Aldon Lifecycle Manager (LM) may be used to develop products that fall under the requirements of HIPAA, the underlying code of those products (i.e. the data stored in LM) should not itself contain PHI. In the event that LM contains PHI, or that it touches PHI in test environments, relevant HIPAA requirements and the capabilities ALM offers are listed on the following page.

| HIPAA REQUIREMENTS | ALM 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. | Aldon Lifecycle Manager and its associated modules (Lifecycle Manager IBM i Edition (LMi), Lifecycle Manager Enterprise Edition (LMe), Community Manager (CM), and Security Service Manager) support unique user IDs for all individuals accessing the systems.<br>Detailed, customizable role-based access levels allow an organization to define the exact capabilities of each system user. Permissions are granular to support any organization's business needs according to the rule of least privilege and segregation of duties.<br>Reports are available showing all users with their associated access capabilities. |
| **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. | The Aldon CM module supports automated, system-driven workflows that may include access request, authorization, and provisioning processes.<br>Reports are available showing all administrative activity performed within the system, including the modification of user access and roles. |
| **Security Awareness and Training: 164.308(a)(5)**<br>Implement a security awareness and training program for all members of its workforce (including management). | The Aldon CM module supports automated, system-driven workflows that may include information security training programs. |
| **Facility Access Controls: 164.310(a)(1)**<br>Implement policies and procedures to limit physical access to its 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 prem, and the organization can implement physical and environmental controls as with all other computing equipment. |
| **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). | Aldon Lifecycle Manager and its associated modules (Lifecycle Manager IBM i Edition (LMi), Lifecycle Manager Enterprise Edition (LMe), Community Manager (CM), and Security Service Manager) support unique user IDs for all individuals accessing the systems.<br>Detailed, customizable role-based access levels allow an organization to define the exact capabilities of each system user. Permissions are granular to support any organization's business needs according to the rule of least privilege and segregation of duties. |
| **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 actions performed within the system, including accessing or modifying data, is logged and auditable. |
| **Integrity: 164.312(c)(1)**<br>Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | Access to modify data is restricted to users specifically authorized within that development release and environment.<br>All changes made to code are highlighted by the Aldon Harmonizer module, allowing the organization to validate that all changes were made in accordance with an approved work order. |
| **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. | Passwords are required for users to access each system. Aldon LMi also supports integration with IBM i user credentials, and Community Manager supports LDAP integration with Active Directory credentials. |
| **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. | Users access the web-based LMe, Security Service Manager, and CM systems using encrypted HTTPS sessions. Aldon LMi utilizes encrypted SSH sessions.<br>All data in transit, including code being checked in or out or moved to new environments, is encrypted. |

Rocket


201609CSRALMV1