



The Security Division of EMC

RSA Solution Brief

RSA enVision® Platform: Helping to Enable Protected Health Information



Security is a top Healthcare CIO priority, with nearly 1 in 4 reporting a security breach in the last year.* In order to achieve compliance with PHI requirements, healthcare providers, health plans and healthcare clearinghouses, as well as their business partners, must have the systems in place to capture, collect and protect all the data needed for those reports, as required by healthcare regulations.

Objectives to Meet PHI Compliance

Protected Health Information (PHI), under the U.S. Health Insurance Portability and Accountability Act (HIPAA), is any information about health status, provision of health care or payment for health care that can be linked to an individual. This includes any part of a patient's medical record or payment history. And the Joint Commission recommends that as healthcare organizations acquire information systems, they should require capabilities that provide a high level of security and confidentiality protection including: encryption, detailed user access controls, transaction logs and blinded files.

Directives 95/46/EC set up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each member state set up an independent national body responsible for the protection of this data.

Healthcare organizations have a regulatory responsibility to ensure privacy and security of patient PHI. To meet PHI compliance requirements, healthcare organizations must protect information from reasonably anticipated threats to security and integrity, as well as the unauthorized use or disclosure of that information. They must also ensure that their workforce complies with the requirements and that confidentiality is maintained.

To achieve these objectives, the following information is required for reporting and retention purposes:

- **Access Control** monitors attempts to access anything on the organization's system, including files, directories, database records or applications.
- **Configuration Control** monitors the configuration, policies and software installed on systems covered by a particular compliance regulation and all systems with access to that system.

At a Glance

- Provides for the collection and protection of *All the Data™* needed for a number of reports required for PHI including Health Insurance Portability and Accountability Act (HIPAA), Joint Commission, and EU Data Protection Directives 95/46/ EC which protect the processing of personal data and free movement of such data.
 - Analyzes both real-time and historical data and presents information in views and reports designed to meet the far-ranging needs of your healthcare organization.
 - Provides the ability to automatically generate alerts based on non-compliance with an observed baseline.
-
- **Malicious Software** capabilities detect, collect and report malicious activities caused by viruses or other malicious code.
 - **Policy Enforcement** verifies that all users are complying with regulations to reduce the chance of accidental exposure of sensitive information.
 - **User Monitoring and Management** creates a complete audit of the activities of non-employees with access to private data and takes steps to minimize the risk from compromised accounts.
 - **Environmental and Transmission Security** involves the ongoing monitoring of the environment to ensure that security threats are detected and corrected as quickly as possible.

Additional monitoring is required to ensure that the transmission of sensitive data is secured and done with the proper encryption levels.

For more than 1,200 organizations – including some of the largest global Fortune 100 enterprises – the RSA enVision platform is providing a single, integrated 3-in-1 log management solution for simplifying compliance, enhancing security and risk mitigation, and optimizing IT and network operations.

To achieve and maintain compliance in those areas, organizations must use the following functions with respect to the data collected by the RSA enVision™ log management solution:

- Collect, protect and store data in a non-filtered, non-normalized fashion that is preserved in its original format in an efficient and protected manner.
- Establish baseline levels of activity for the entire system and network environment to define “normal activity” and detect unusual levels of activity.
- Report summary and detailed reports for the mandated periods of time.
- Alert organizations to deviations from baseline activities and complex patterns of activity across multiple, disparate devices.
- Vulnerability and asset management capabilities streamline the process of risk mitigation to ensure that valuable resources are deployed on high-confidence threats (rather than false-positives).
- Interactive system analysis to correct policies and settings on systems and provide a granular view of all changes and the effect they have on the environment.
- Establish Incident management capabilities for close monitoring and correction of violations to make sure they are recorded, escalated and corrected in a timely and thorough manner.

These functions ensure that the administrative, physical and technical control demanded by HIPAA and other regulations is maintained. RSA enVision solutions address many of the technical standards required.

The RSA enVision Internet Protocol Database


Using the advanced RSA enVision LogSmart® Internet Protocol Database (IPDB) architecture – deployed in more than twelve hundred enterprises worldwide – the platform is able to capture *All the Data™* from network, security, host, application and storage layers across the enterprise. The LogSmart IPDB analyzes both real-time and historical data and presents information in views and reports designed to meet the far-ranging needs of everyone in your organization – from the IT department to the security department to the compliance and risk officers and executive management.

The benefits of the LogSmart IPDB include:

- Optimal architecture for storing and analyzing unstructured data (unlike a relational database) without any filtering or data normalization
- Maintains a digital chain of custody for all data which assures that once data is committed to the database, it can never be altered – unlike most data schemas used in RDBMS-based solutions
- No agents are required
- Distributed peer-to-peer architecture enables high scalability and performance
- Processes data in parallel so that it can be collected and analyzed at high speed

Compliance Alerts

The RSA enVision platform provides the ability to automatically generate alerts based on non-compliance with an observed baseline. This means, should a particular control deviate above certain thresholds, an alert can be triggered and action can be taken to maintain compliance.



RSA is your trusted partner

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

©2008 RSA Security Inc. All Rights Reserved. RSA, *All the Data*, enVision, LogSmart and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

PHI SB 0508



The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com