



The Security Division of EMC

RSA Solution Brief

Improving Information Security for Healthcare Providers

The impact of the American Recovery and
Reinvestment Act of 2009 (ARRA)



The ARRA provisions relating to health information technology – the HITECH Act (Health Information Technology for Economic and Clinical Health) have allocated more than \$20B of funding to modernize health IT.

In addition, ARRA HITECH has developed new HIPAA privacy, security and protection requirements to advance the secure use of Health IT (for example electronic health records) and further develop secure Healthcare IT Infrastructure for regional health information organizations and health information exchanges.

The new provisions have significantly impacted the breach notification now required for disclosure of PHI and PII, and increased the penalties for violation. In addition, the definition of a *business associate* under HIPAA has been amended to include vendors of personal health records, which were previously not covered under the HIPAA provisions and were monitored only by the FTC.

Whether your healthcare organization is beginning to implement modules of the EHR or is in the process of transforming electronic care processes across your enterprise, EMC and its partners offer solutions that provide the highest levels of performance, availability, security and integration to help meet end user needs. From integrated delivery networks, academic teaching hospitals, medical centers, public health, community hospitals, ambulatory clinics, physician practices and regional health information organizations to health information exchanges, EMC provides a portfolio of solutions to jump start your Electronic Health Record adoption. Within this portfolio, RSA offers advanced solutions to enable healthcare organizations to comply with enhanced HIPAA requirements and to fully protect and secure PHI and PII throughout the healthcare environment.

The provisions have significantly impacted the breach notification now required for disclosure of PHI and PII, and increased the penalties for violation.

Information Risk Management for PHI and PII

The Information Risk Management for Protected Health Information (PHI) solution offers an information-centric approach to security that empowers healthcare organizations to meet the demanding needs of patients, physicians, contractors and other healthcare staff by mitigating risks to PHI and PII, controlling costs, building patient trust and helping to enable compliance with new HIPAA security requirements, all while delivering high quality, safer patient care.

Taking a strategic approach to information risk management and managing the potential risks as confidential patient and clinical data passes through its information lifecycle involves a four-step process:

1. Discover and classify sensitive data: PHI and PII is prevalent and widely distributed throughout the healthcare environment – on clinical workstations, USB flash drives, networks, electronic health records, applications, patient portals, etc – and a healthcare organization needs to classify and discover all instances of confidential data in order to be able to put in place policies and enforcement controls to protect that data from security risks.

The RSA® RiskAdvisor service determines where sensitive data resides across the healthcare environment and the security risks it is exposed to. It identifies relevant policies, procedures, and controls to address those risks.

The **RSA® Data Loss Prevention Suite** discovers, monitors and protects PHI and PII from data loss or misuse, whether in a data center, on the network or out at the end points

2. Define policies to determine how PHI and PII should be protected – such as who can access the data, where can they access it from and what can they do with it.

The **RSA Information Security Policy Development** service helps healthcare organizations to define and map policies (the rules for appropriate handling of PHI) to best practices, individual business requirements and applicable regulations such as HIPAA. Policies should include which employees, clinicians, patients and other users and applications are authorized to access this data and how, when and from where they are allowed to access it. For example, physicians might be provided access to the entire patient record at all times and from all locations, but other clinical staff may only be able to access specific lab data or selected clinical department data on a patient – and only during specific hours and from within the firewall.

3. Select and enforce controls by establishing a control framework to enforce policy. A comprehensive control strategy will include a combination of data and access controls

Data controls manage the PHI and PII itself and are especially effective in collaborative environments where data is always being created, shared and transformed. Data controls include products and technologies such as the RSA Encryption & Key Management Suite, RSA Data Loss Prevention, and Information Rights Management.

Access controls include both authentication (i.e., is the user who he or she claims to be?) and authorization (i.e., what can the user do once he or she gains access?). Access control logs are key in demonstrating compliance with policy and/or regulations.

RSA SecurID® authentication provides strong two-factor authentication – in hardware or software formats - to identify legitimate users for secure access to clinical resources.

RSA® Access Manager – a web-access management solution that enables healthcare organizations to cost-effectively provide secure access to web applications, such as patient & physician portals – controlling authentication and authorization of “who has access to what”.

RSA® Adaptive Authentication is a comprehensive authentication and risk management platform that monitors and authenticates physicians and other staff to clinical applications, without the requirement to carry hardware authenticators

4. Monitor, report and audit compliance with internal security policy and industry regulations such as HIPAA.

The **RSA enVision®** platform automatically collects, manages and analyses event security logs and real-time events from the healthcare infrastructure. These logs monitor systems and keep a record of security events, information access and user activities for real time and forensic analysis, and provide detailed reporting to demonstrate compliance with internal policy or external regulations such as HIPAA.

RSA is your trusted partner

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, 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/healthcare.



©2009 RSA Security Inc. All Rights Reserved.
RSA, SecurID 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.

ARRA_SB_0509



The Security Division of EMC

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