RSA SECURE WEB ACCESS FOR HEALTHCARE ENVIRONMENTS
Security solutions for patient and provider access

AT A GLANCE
Healthcare organizations of all sizes are responding to the demands of patients, physicians, payers and employees for better access to information and services by creating patient and provider websites. These access points are becoming an important part of improving healthcare organizations’ care delivery, patient and physician satisfaction and clinical efficiency by acting as a cost-effective means to increase access to and exchange of clinical data.

Securing web applications and leveraging them as a single point of access to multiple information sources for employees, partners and patients can increase efficiency, reduce costs and present new business opportunities.

As more healthcare organizations deploy web-portal technologies with access to more clinical data, they must satisfy patient concerns by implementing stronger security measures to protect the privacy of patient information. The increasing use of Protected Health Information (PHI) and patient portals are increasing security concerns. Additionally, security measures are needed to not only comply with requirements such as the HIPAA Security Rule and the EU Data Security requirement, but to gain incentives by complying with Health Information Technology for Economic and clinical Health (HITECH) Meaningful Use guidelines for Electronic Health Records (EHR).

Organizations are implementing Electronic Health Records (EHR) and transforming electronic care processes to accelerate service delivery. An important consideration for using and maintaining electronic healthcare information meaningfully is mitigating the potential risk to those records, and managing compliance to relevant regulatory requirements. The increasing use of Personal Health Information (PHI) and patient portals are increasing security concerns. Healthcare consumers are knowledgeable and demand privacy and trust protections for their data. Just as in other businesses, healthcare consumers want safeguards against medical identity theft and fraud.

Web applications to facilitate information exchange, increased communication and flexible access are an integral part of the healthcare industry. Patients are demanding deeper access to their health information. Doctors and healthcare providers need access to sensitive patient information, services and applications in order to expedite patient care and become more efficient. Business partners are looking for tighter integration of processes.

Accompanying the increase of business efficiency and convenience delivered with healthcare web applications are concerns about privacy, secure access management, fraud and increased risk and cost of security breaches. Sensitive information such as EHRs are deployed to user populations through web applications; authenticating users and controlling access heightens the need for security solutions to meet both internal policies and regulatory requirements.

A healthcare organization’s reputation would suffer from negative publicity due to security breaches by unauthorized users. In addition, organizations struggle to balance a security solution’s ease of use with the strong protection mandated for healthcare information. As the number of users grows exponentially, healthcare organizations require mechanisms to reduce the cost and overhead of enrolling and maintaining its user community. RSA Secure Web Access for Patient and Provider Access addresses all of these concerns.
THE RSA SOLUTION

The RSA Secure Web Access solution secures the exchange of sensitive enterprise and personal data via web applications – across multiple users and across heterogeneous environments and domains to provide risk based access controls and strong protection of user credentials. This is accomplished by creating a centralized security service that securely enrolls end users, offers granular authorization policy to control access based on a single source of identity truth, secures the credentials and provides positive, transparent user authentication.

Healthcare organizations can choose from a wide range of authentication, deployment and customization options to fit their unique security requirements. RSA Secure Web Access for Patient and Provider Access allows healthcare organizations to:

- Secure exchange of sensitive patient health information via physicians and patient portals and mitigate online data breaches
- Confidently enroll new users for quick and easy access to portals - even if no prior relationship with those users exists
- Secure information from loss and unauthorized access with stronger authentication – without frustrating end users
- Enhance compliance
- Achieve quicker clinical decision making and improved patient care by:
  - Accelerating deployment of EHR technologies and applications
  - Providing rapid clinician access to a "single patient view"
  - Streamlining clinical and administrative workflows
- Uniquely protect stored user credentials

The components of the solution include RSA Adaptive Authentication, RSA Access Manager, RSA Adaptive Directory, RSA Distributed Credential Protection and RSA Identity Verification (from LexisNexis). The components may be deployed individually or as a complete solution. Healthcare organizations may also leverage other RSA security and compliance solutions as well as EMC hardware, software and services, and Healthcare Channel Partner applications to complete their information infrastructure needed to store, protect, optimize and leverage patient information safely and securely.

Between 2005 and 2008, nearly 230 million electronic records were breached including almost 39.5 million electronic health records. i

In a November 2011 survey completed by 72 provider organizations conducted by Ponemon Institute, 96% reported having had at least one data breach in the past 24 months. ii

A thief downloading and stealing data can get $50 on the street for a medical identification number compared to just $1 for a Social Security number. For those receiving the medical ID number and using it to defraud a health care organization, the average payout is more than $20,000, according to Pam Dixon, executive director of the World Privacy Forum. Compare that to just $2,000 for the average payout for regular ID theft. iii
RSA ADAPTIVE AUTHENTICATION
RSA Adaptive Authentication is a comprehensive authentication and risk management platform providing cost-effective protection for an entire user base. Adaptive Authentication monitors and authenticates user activities based on risk levels, institutional policies and customer segmentation and can be implemented with most existing authentication methods including invisible authentication, out-of-band authentication, challenge questions and the multi-credential framework.

RSA ACCESS MANAGER
RSA Access Manager enables organizations to centrally manage authentication and authorization policies for a large number of users accessing web applications and portals. Access Manager empowers enterprises to deploy applications more quickly while providing seamless user access with single sign-on. Access Manager supports a wide range of authentication methods, including RSA Adaptive Authentication, RSA Identity Verification and RSA SecurID.

RSA ADAPTIVE DIRECTORY
RSA Adaptive Directory delivers a global view of identity on top of existing identity infrastructure. It uses model-driven virtualization to externalize identity out of disparate data silos into a common, interoperable service. Users who exist in more than one source now have a single profile of all attributes without duplication. A flexible identity service is critical to enabling any initiative requiring secure access to a global list of users, along with their complete identity profiles—including RSA web access management, authentication, identity federation and fine-grained authorization.

RSA DISTRIBUTED CREDENTIAL PROTECTION
RSA Distributed Credential Protection scrambles, randomizes and splits passwords into two servers, removing the primary points of compromise that attackers are targeting. User credentials are strongly protected, but even more, if one server is breached, Distributed Credential Protection is designed to help ensure that both authentication decisions and secrets remain secure. With the ability to proactively re-randomize secrets, credentials can be re-randomized before the attacker can breach the other server. Even if the other server is breached, because the secrets have been re-randomized, the stolen data is useless.

RSA IDENTITY VERIFICATION
RSA Identity Verification, from LexisNexis, is a strong consumer authentication and fraud prevention service that validates user identities in real time, reducing the risk of identity impersonation. Using Dynamic Knowledge-Based Authentication, Identity Verification challenges users with a series of top of mind questions generated from billions of public and commercially available records.

RSA is the only vendor who can offer an end-to-end portal security for healthcare environments, allowing you to deploy once for multiple applications. Accelerate your security deployment and increase the number of applications that are protected by Adaptive Authentication by combining it with Access Manager and Identity Verification. Securing a portal from enrollment to authentication to authorization allows portals to reach their full potential without being bogged down by security concerns and reducing password reset costs and complexities.
RSA Secure Web Access provides a secure end-to-end framework for web access for physicians, patients, payers and employees as well as compliance to regulations. Enable convenient information exchange while protecting against sensitive and expensive data breaches.

**REGULATIONS**

HIPAA Security Rules governing electronic Protected Health Information (ePHI) specify confidentiality, integrity and availability for any Covered Entity that creates, receives, maintains and transmits ePHI. Healthcare organizations must:

- Protect against reasonably anticipated threats to the security or integrity of information
- Protect against reasonably anticipated uses and disclosures not permitted by HIPAA Privacy Rules
- Ensure compliance by workforce

The Joint Commission requires healthcare organizations to use information systems that provide a high level of security and confidentiality protection, including encryption, detailed user access controls, transaction logs and blinded files that address the following needs:

- To leverage technology to solve special privacy issues, such as restricted access
- For existing technology to set levels of authorization for access to patient data according to the role the user plays in a patient’s care
- To maintain and routinely analyze records of all accesses and/or modifications to personal health information

The Health Information Technology for Economic and Clinical Health (HITECH) Act provides HHS with the authority to establish programs to improve health care quality, safety, and efficiency through the promotion of health information technology (HIT), including electronic health records and private and secure electronic health information exchange. Under HITECH, eligible health care professionals and hospitals can qualify for Medicare and Medicaid incentive payments when they adopt certified EHR technology and use it to achieve specified objectives.

Two regulations have been released, one of which defines the “meaningful use” objectives that providers must meet to qualify for the bonus payments, and the other which identifies the technical capabilities required for certified EHR technology.

- Incentive Program for Electronic Health Records: Issued by the Centers for Medicare & Medicaid Services (CMS), this final rule defines the minimum requirements that providers must meet through their use of certified EHR technology in order to qualify for the payments.
- Standards and Certification Criteria for Electronic Health Records: Issued by the Office of the National Coordinator for Health Information Technology, this rule identifies the standards and certification criteria for the certification of EHR technology, so eligible professionals and hospitals may be assured that the systems they adopt are capable of performing the required functions.
CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.


EMC2, EMC, the EMC logo, [add other applicable product trademarks in alphabetical order] are registered trademarks or trademarks of EMC Corporation in the United States and other countries. VMware [add additional per above, if required] are registered trademarks or trademarks of VMware, Inc., in the United States and other jurisdictions. © Copyright 2012 EMC Corporation. All rights reserved. Published in the USA. 06/12 Solution Overview HSWA612

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice. www.EMC.com/rsa