



The Security Division of EMC

RSA Solution Brief

## **RSA Secure Web Access for Patient and Provider Portals**

Security Solutions for Healthcare  
Environments



# Business Challenges

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 portals. These portals 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.

As more healthcare organizations deploy web-portal technologies with access to more clinical data, they must implement stronger security measures to protect the privacy of patient information to satisfy patient concerns. Additionally, security measures are needed to meet HIPAA access control requirements, to maintain Joint Commission (JCAHO) accreditation and to meet EU Data Security requirements.

A healthcare organization's reputation may also 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 Portals addresses all of these concerns.

---

## Solution Description

---

The Secure Web Access for Patient and Provider Portals solution secures the exchange of health information via web applications across diverse environments. This is accomplished by creating a centralized security service with the ability to enroll new users, authenticate with the appropriate level of security and authorize access. RSA Secure Web Access for Patient and Provider Portals creates a secure framework for web access to Protected Health Information (PHI).

## Solution Value

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 Portals allows healthcare organizations to:

- Secure exchange of sensitive patient health information via physician and patient portals,
- Confidently enroll new users even if no prior relationship with those users exist,
- Secure information from loss and unauthorized access with stronger authentication – without frustrating end users,
- Manage access to patient health information and
- Enhance compliance and mitigate online data breaches.

The components of the solution include: **RSA® Identity Verification from Verid**, **RSA® Adaptive Authentication** and **RSA® Access Manager**. 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 best-in-class 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.

**RSA® Identity Verification from Verid** is an advanced platform that incorporates knowledge-based authentication (KBA) to help streamline the enrollment process by providing real-time confirmation of user identities. Users are presented with a series of top-of-mind questions utilizing relevant facts on the individual obtained by scanning billions of public records. RSA Identity Verification is able to deliver a confirmation of identity within seconds, without requiring any prior relationship with the user.

RSA® Adaptive Authentication provides a balance between security and usability with authentication options for secure access control policies. Risk-based authentication meets the growing needs of healthcare organizations to protect web portals with access control and provides an authentication mechanism that best suits the needs of the organization and its patients. It incorporates a range of parameters behind the scenes – including device and network forensics, behavioral analysis and the end user’s computer itself as a second authentication factor – to ensure positive identification.

RSA® Access Manager centralizes access controls from a single administrative console, enabling organizations to manage “who has access to what” with the ability to delegate specific privileges to groups or departments. It provides a centralized authorization and authentication engine delivering end user convenience while significantly enhancing security and privacy controls. Healthcare organizations can stay ahead of industry requirements governing who has control and access to PHI.

**Getting Started**

To learn more about RSA Secure Web Access for Patient and Provider Portals from EMC, please contact your EMC or RSA account manager, or visit [www.emc.com/healthcare](http://www.emc.com/healthcare) or [www.rsa.com](http://www.rsa.com).

RSA Secure Web Access for Patient and Provider Portals provides a secure end-to-end framework for web access for physicians, patients, payers and employees.

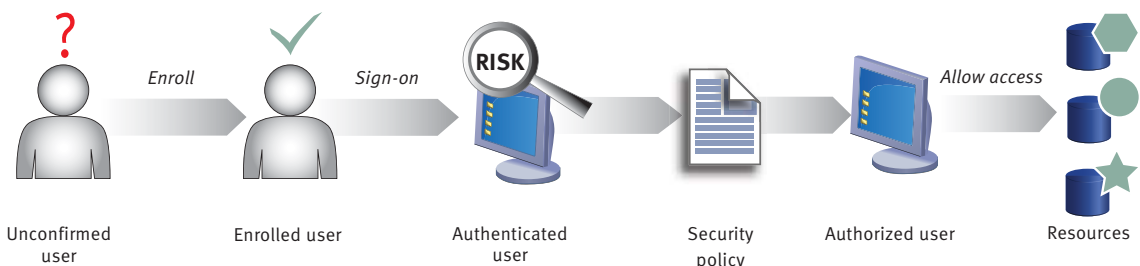
HIPAA Security Rules governing Protected Health Information specify confidentiality, integrity and availability for any Covered Entity that creates, receives, maintains and transmits electronic patient information. Healthcare organizations must:


- Protect against reasonably anticipated threats to the security or integrity of information,
- Protect against reasonably anticipated uses and disclosures not permitted by privacy rules, and
- Ensure compliance by workforce.

**Joint Commission Security Requirements**

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.





## 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](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).

©2007 RSA Security Inc. All Rights Reserved.  
RSA 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.

SWAP SB 1107



The Security Division of EMC

RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)