calgary / scientific

ENSURING YOUR ENTERPRISE IMAGE-VIEWER IS FULLY SECURE

Ensuring the security of information and applications is a critical priority for all organizations, particularly those in the healthcare field. The architecture and features of the right enterprise image-viewer enable medical images and information to be securely and conveniently accessible to users from anywhere in the world, without compromising network or information security.

This guide describes strategies to ensure your enterprise images are fully secure, even when you provide the flexibility of mobile health solutions to practitioners.

Healthcare Breaches and Costs

Data security continues to be a major health IT concern. A study conducted in 2012 by the Healthcare Information and Management Systems Society (HIMSS) found that 34% of respondents named security breaches as a top concern, and 23% said their organizations experienced a breach in the last year.[1]

This concern is only increasing with the use of mobile devices in healthcare. Devices are being used to access patient records and if downloaded data were to ever go missing, it would put the hospital at huge risk. Best practice is to ensure that patient data never reaches the end device. It is equally important to manage devices that are brought in from a users home.[2][2a]

There are countless ways for there to be a breach with patient data, from laptops or mobile devices being stolen to passwords being leaked. HIPAA violations can range from $50,000 to $1.5 million in fines, with a recent case reaching a record setting $4.8 million in fines.

Steps to Protect Your Enterprise

More employees are starting to use mobile devices for business purposes across every industry, providing convenience and flexibility. However, mobile devices continue to be a significant source of data breaches. To help with mobile security, organizations should:

1. Educate staff on the importance of mobile security.
2. Use security features on devices.
3. Put network security policies in place.
4. Use authentication for all users.
5. Use secure connections.
6. Ensure that your solution has built-in encryption and user authentication - secure LDAP and Active Directory, that can be fully integrated into your IT policies and infrastructure.
7. Ensure they are using an enterprise viewer that is completely secure.

[1] Source: http://www.rheumatologynetwork.com/practice-management/your-patient-data-secure
[2] Source: http://www.onesourcedoc.com/blog/bid/95168/10-Examples-of-HIPAA-Violations
[2a] Source: http://www.hhs.gov/news/press/2014pres/05/20140507b.html

Calgary Scientific Approach to Security

Security has been part of the design of our enterprise image-viewing solution, ResolutionMD, since its inception. The solution ensures a fully secure experience in the following ways:

1. No patient data is actually left persistent on the client mobile device or browser session. Once a session times out or is ended, the data in memory is deleted and no data is persistent on the device. If a phone or tablet is lost or stolen there is no concern about patient data being left behind and accessible.
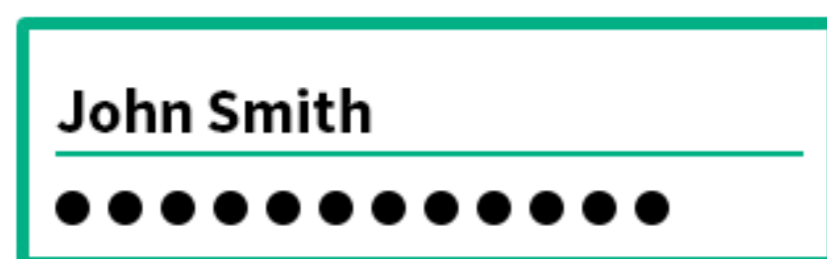
2. The ResolutionMD server is set up to require clients to enter login credentials for production use.

3. The ResolutionMD client is typically further secured with the use of SSL. SSL implemented in conjunction with the ResolutionMD Server ensures that all data transmission between the client device and the server are encrypted so as not to be interpreted while in transit from a network.
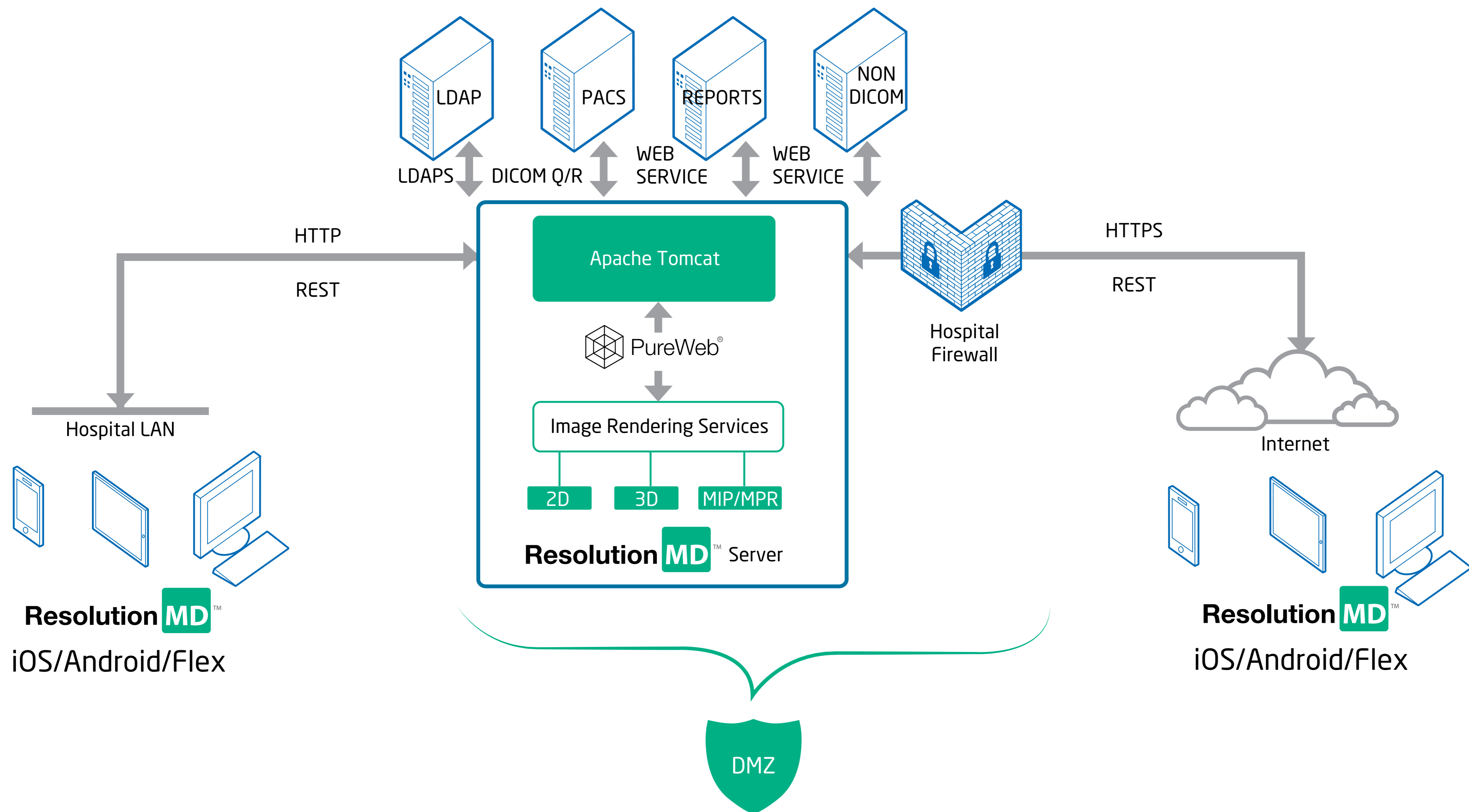
4. Optionally, a VPN can be added as a secure conduit through which the end user device can communicate with the ResolutionMD server.

Other solutions will send patient data to the end-user device, allowing easy access to that data if the devices are stolen. In some cases, data is not being left on the device, but is being rendered on the users laptop or mobile device which can lead to data being left in the memory. Some solutions are not integrated into the IT environment and require additional or different passwords to access the application and the data. This means that if a device goes missing IT departments have no control over the access and cannot shut down the breach.

As mentioned above, ResolutionMD does not download data to any device and is 100% secure.

ResolutionMD Architecture

LDAP

PACS

REPORTS

NON DICOM

LDAPS

DICOM Q/R

WEB SERVICE

WEB SERVICE

HTTP

REST

Apache Tomcat

PureWeb®

Image Rendering Services

2D

3D

MIP/MPR

Resolution **MD**™ Server

HTTPS

REST

Hospital Firewall

Internet

Hospital LAN

Resolution **MD**™

iOS/Android/Flex

Resolution **MD**™

iOS/Android/Flex

DMZ

Images are queried from the PACS on demand, with no images being stored on the ResolutionMD server. Images are then rendered and made available for display to the end user device. This keeps the patient data safe behind the firewall. Users are authenticated against the site LDAP for full integration into IT policies.

"

Mobile solutions can empower caregivers, enhance efficiency and improve patient care, but only if healthcare data remains protected at all times. With Calgary Scientific's ResolutionMD as part of the cloud-based Dell Unified Clinical Archive, physicians can securely view images and render a diagnosis from any web or mobile device across the enterprise or even outside the walls of the hospital.

Sid Nair
Vice President/General Manager
Healthcare and Life Sciences at Dell Services

"

Resolution MD ®
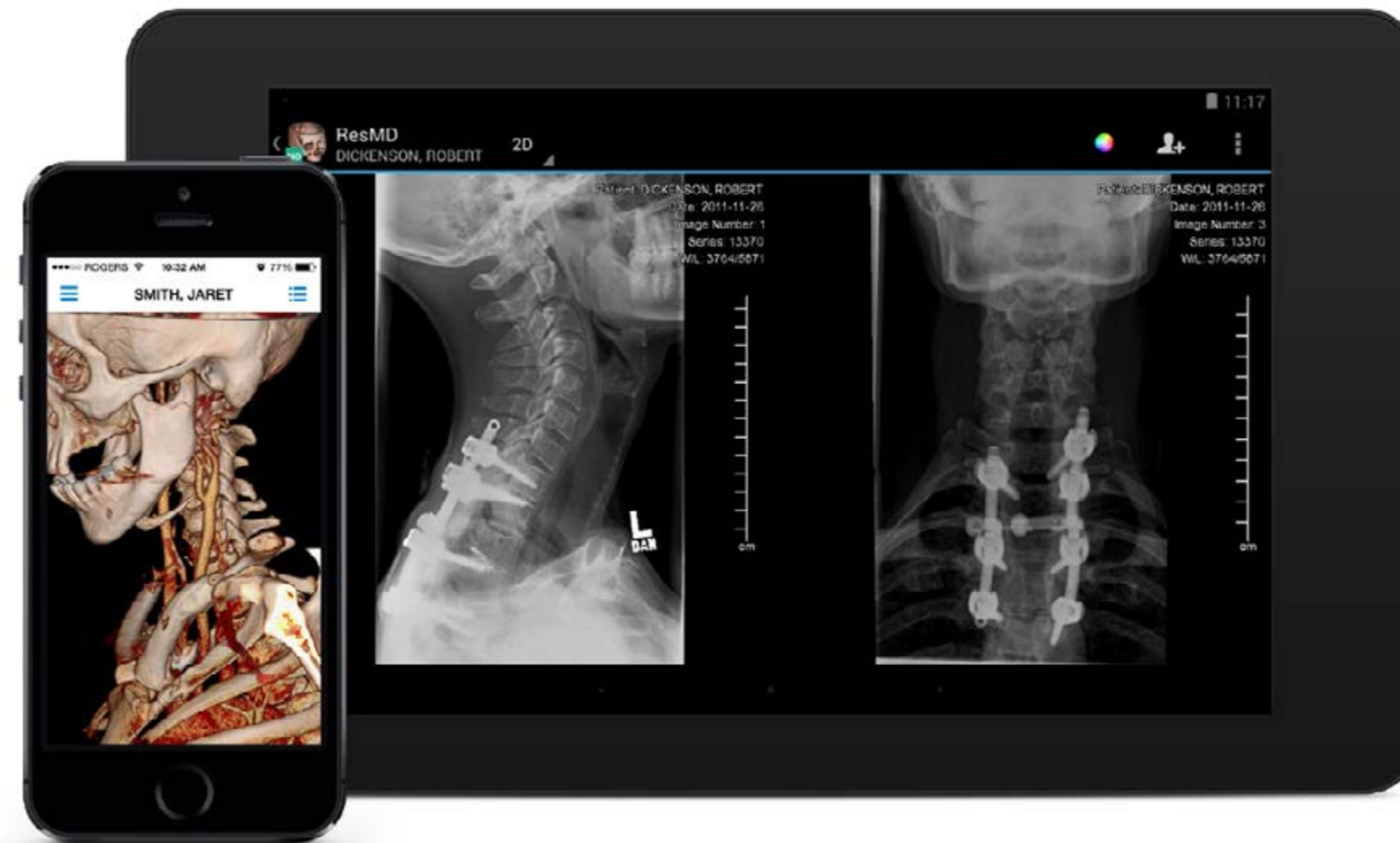
ResolutionMD enables doctors to securely view patient images and reports from a wide variety of computers and mobile devices, collaborate with other practitioners and diagnose from any location. Whether you are a single facility or a large healthcare system with tens of thousands of users, ResolutionMD is the best choice for seamless image access across multiple departments. The FDA cleared, CFDA registered, Health Canada licensed and CE marked mobile medical diagnosis software can be integrated into any EMR and easily plugs into existing distributed storage systems. ResolutionMD's federated approach is an important differentiator from other solutions as highly sensitive data is never moved to a device and no additional data storage locations are created. ResolutionMD is currently installed in leading healthcare institutions around the world via a network of more than 45 world class healthcare partners. To see ResolutionMD in action, access the self-serve demo.