HIPAA Security: Defense in Depth

"Better, Faster, and Cooler..."

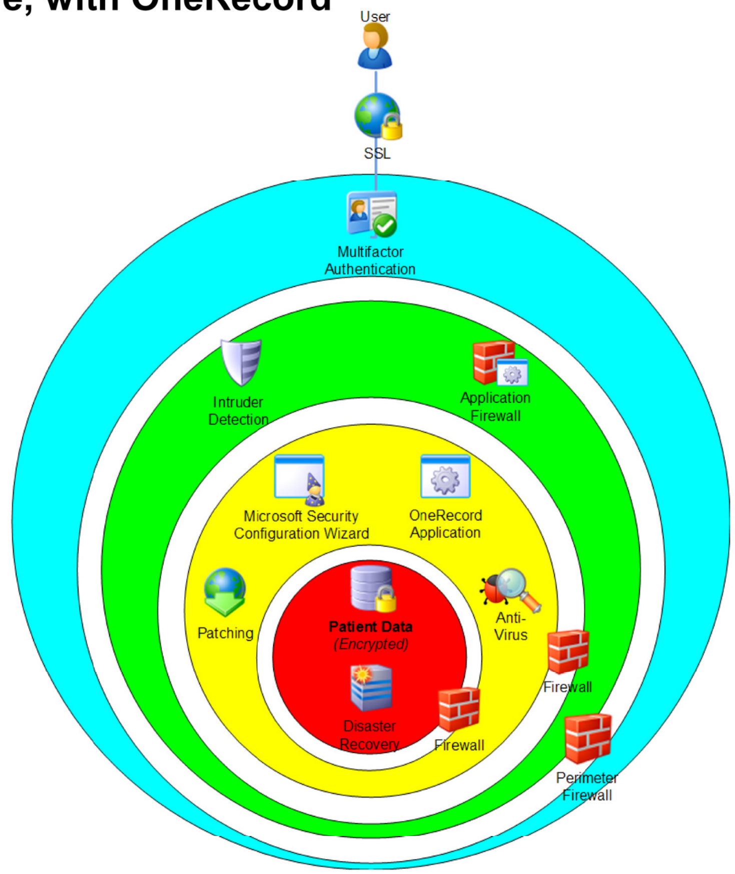
-RelWare Infrastructure

Accessibility, performance, and scalability of your EMR is not enough.

An enterprise-worthy EMR application will provide peace of mind that your patient data is secure.

OneRecord accomplishes all of these things.

Achieve Peace of Mind that Your Patient Data is Secure, with OneRecord



HIPAA

Part of providing excellent patient care is also protecting the privacy of all confidential patient medical records. HIPAA defines very clear requirements that must be met to adequately secure patient health information from unauthorized access. RelWare takes the security of patient data very seriously. From the network infrastructure to the OneRecord application, all decisions regarding handling of patient data center around making it accessible only to those with the appropriate permissions.

Defense in Depth

RelWare practices the Defense in Depth approach to securing systems by providing multiple layers of defense throughout the OneRecord environment.
Monitoring is done at all levels: software, server, device, and network.

Physical Security

When hosted with the RelWare SaaS model OneRecord is housed at a Tier III facility guaranteeing 99.99% uptime. The data center floor is accessed and tracked via swipe card and key code by limited personnel. Racks are locked except when direct hardware access is needed, and then, again, by only a very few certified IT staff members.

OneRecord™

RelWare®

Authentication

Multi-factor authentication is used to validate users. Both personal and technical factors, such as a username/password combination and a token, can be used to authenticate users.

Password policies are used to enforce complexity, limit duration, forbid reuse, and block accounts that fail too many login attempts.

SSL is used to encrypt all connections. Data is encrypted from the end user device to the OneRecord data repository and back again.

Perimeter Security

The perimeter provides an entry point for access to OneRecord by users, as well as to servers by IT personnel providing support. A perimeter firewall ensures that only legitimate traffic is let in to OneRecord. All other traffic is blocked.

OneRecord traffic is also filtered through an application firewall. The application firewall validates each request and drops any suspicious requests.

An Intrusion detection system (IDS) is used at the perimeter to detect attacks and attempts to gain access to OneRecord. The system analyzes network traffic looking for malicious traffic, such as DOS attacks and port scans. If any suspicious traffic is detected, operators are immediately notified.

Network Security

The core infrastructure uses multiple VLANs to segment and secure network traffic. This separates server traffic from HL7 traffic. It also ensures that the only entry points into the application are available only to the systems that use them. For example, HL7 traffic can access only the interface servers on the HL7 network segment. No other servers are on the HL7 network segment.

Server Security

The servers utilize the Security Configuration Wizard of Windows Server™ 2008 to ensure that the only services that are running on the servers are needed.

Server firewalls allow only ports that are required and block everything else. Firewall rules are dependent on network segments.

Detailed logs are kept on all servers and are stored off the local system. Regular reviews of the logs make sure not a single system has been compromised.

Servers are patched regularly. Patches are thoroughly tested before being approved for production systems. Systems are validated to ensure a patch level before they can be used.

Anti-virus software is implemented on the servers to protect servers against malicious software. Strict anti-virus policies are used to protect servers without the risk of data corruption.

Data Security

OneRecord database servers use transparent data encryption (TDE). TDE encrypts entire databases to make sure PHI is protected without a noticeable performance impact.

Because of TDE, all data backups are already encrypted. Once transferred to tape, backups are moved offsite and stored in a secure storage vault.

Database traffic is separated to the innermost network segment. That means patient data is at the core of the system and protected by multiple layers of security.

About RelWare Technology

At RelWare, we realized in 1998 that the Internet, and specifically, Web-based technology was the future. We built our company with the continued motto: “Every application is a Web application.” This meant that anytime we looked at writing a new application, we first asked ourselves, “Can I write this as a Web application?” What we soon found was the answer was invariably “Yes”. . .every time.

It has been 10 years since we started, and we are still saying “Yes”. . .every time.