Electronic medical records solution brief

Security Rx for your electronic medical record system

Amidst the complex, ongoing process of healthcare reform, one dramatic change is already here: a new mandate for Electronic Medical Records (EMR). An EMR is a digital patient health record used for real-time clinical care, billing and reporting. Use of EMR systems is rising in large healthcare institutions, and requirements in the recent economic stimulus act will eventually make these systems pervasive in healthcare providers of all sizes. The Act also makes protecting electronic patient health information a top priority. This article shares ideas for securing EMR systems by leveraging existing security processes and technologies.

The mandate for EMR was signed into law on February 17, 2009 by President Obama in the American Recovery and Reinvestment Act (ARRA). It establishes a national health information technology infrastructure, and directs the adoption, use and exchange of "electronic health records" (EHR) to improve health care quality, safety, and efficiency.

The Act also directs the creation and use of health IT standards, mandates privacy rules for the safety of electronic health records, and creates incentives for adoption and meaningful use of certified EHR technology.[1]

Who is affected by EMR

Provisions in the Recovery Act affect all healthcare providers—especially IT professionals who deploy and manage security of healthcare systems and data.

[1] The terms EMR and EHR are interchangeable. EMR is common in the IT industry, while EHR is typically used in a legislative context.

It is likely the IT-related impact of this Act will rival the Health Insurance Portability and Accountability Act (HIPAA), so you will hear a lot about EMR in the near future.

Luckily, its provisions do not replace security and privacy requirements of HIPAA, which means you can leverage your organization's existing foundation of processes for HIPAA toward securing the new world of EMR systems.

Inside an EMR system

Physician offices, hospitals and other healthcare organizations can implement an EMR system with multiple levels of functionality. Basic categories include health information and data such as patient demographics, problems, medications and clinical notes. Order entry management includes prescriptions, lab and radiology orders. Results management includes various reports and imaging. The clinical decision support category includes drug and allergy warnings, and other guidelines. Population health management includes public health reporting and notification of diseases.

While many of these EMR applications may be new to your organization, there is a familiar common denominator: each uses a database and EMRs are accessed and used over a network. Many applications are Web-based. EMR sharing and exchange occurs internally over the provider's network, and by externally authorized people and organizations via private and public networks, including the Internet.

Why EMR? Why now?
Electronic medical records offer many benefits:

- Provide instant medical data to emergency responders, especially for travelers whose doctors are in another city or state
- Improve healthcare with accurate, timely personal health data
- Reduce medical errors caused by not coordinating actions with a patient's health data
- Improve coordination of individual healthcare between multiple providers
- Help response to urgent public health threats
- Facilitate health and clinical research
- Improve healthcare options for consumers

First requirement: Security of EMRs

The first-stated responsibility in the Act is for a new nationwide health information technology infrastructure that "ensures that each patient's health information is secure and protected, in accordance with applicable law." Security is identified before improving healthcare, reducing errors, lowering costs and all the rest of the Act's purposes. Thus, as an IT security professional, your personal mandate is a vital, highly visible part of ensuring the success of EMR systems.

Given that EMR systems use databases and networks, your familiarity with traditional security controls will go a long way toward protecting the new genre of electronic medical systems. By the end of 2009, standards for health IT will begin to specify technologies and certification mechanisms. Fleshing out specifics will be a longer process.

The Act directs involvement of the National Institute of Standards and Technology (NIST), and it is likely NIST will leverage its well-known security standard: Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations. This standard includes 205 controls for security and program management spanning 17 families or areas for comprehensive protection of information and networks. EMR systems use underlying technologies that leverage many of these security controls.

Protecting stored EMRs

Physicians, hospitals, pharmacies, medical suppliers and related healthcare organizations need to protect the safety of EMRs stored in databases and applications operating onsite. The Act mentions required use of two specific security technologies (although others may be expressed in forthcoming healthcare IT standards from HHS):

- Authorization and authentication for access control; and
- Technologies or methodologies for rendering health information unusable, unreadable, or indecipherable—usually implemented with encryption.

EMRs require the protective mechanisms provided by a role-based access control system and its associated fine-grained permissions that regulate who are authorized to see specific data in each patient medical record. Some of these controls will be integrated within EMR applications, but these are a backstop to the standard frontline network access and identity management controls in VLANs, VPNs, and next-generation firewalls.

Encryption is a key security technology for data at rest. If an unauthorized individual somehow manages to reach the data store, encryption ensures that EMR data is unreadable.

One area that is often overlooked is data stored in a backup and disaster recovery system. Your organization will want to encrypt that data as part of comprehensive security for EMRs. Use strong encryption technology such as 3DES and AES for the best protection of stored EMRs.

Protecting EMRs in transmit

Data breaches can come from external sources using the network as an access mechanism. Breaches can also occur by insiders, including rogue employees and contractors who are already "trusted" users inside the network boundary. Since breaches can be two-way, EMR security must extend beyond data loss prevention by including a variety of network controls such as firewalls, intrusion prevention, anti-virus and anti-spyware. Another important control is use of a Web Application Firewall to prevent exploitation of web-based vulnerabilities from accessing EMR data. However, there are other security controls with special utility to healthcare organizations.

Wireless is a key example since so many hospitals rely on mobile connectivity where EMRs flow through devices such as patient data entry tablets, mobile carts, or nurse/physician PDAs. Consider using wireless security controls that integrate universal 802.11n/b/g and 3G /4G wireless with your firewall/VPN gateway.

As for VPN, there are strategic considerations for internal vs. external connectivity. IPSec is a desirable technology for managing internal network access to EMR systems because it leverages identities of the people and devices used for access. But use of EMRs typically extends outside your organization to include dynamic connections by people and systems that are not necessarily "known" by your network access controls. For this reason, utilizing SSL VPN technology for remote access adds considerable strength and simplicity to securing those connections and protecting EMR data.

Associated with data loss prevention is stopping unauthorized passage of EMRs via email, and other communications paths over the network. For example, security of email is already a requirement with HIPAA, and EMRs are no different. Data loss prevention entails intelligently monitoring and identifying digital communications and associated EMR attachments that violate compliance policies. Deploying a gateway-based

Financialincentives for EMR deployment

ARRA provides physicians and hospitals up to five consecutive years of payments for deploying EMR.

The maximum cumulative payment is $44,000 per physician. Amounts may vary for hospitals and HMOs.

Recipients must become "meaningful users" of EMRs. Guidelines have been published by the Dept. of Health and Human Services.

A provider will get reduced Medicare payments if it is not a meaningful user by 2014.

Gateway to secure EMRs

Many healthcare organizations have chosen to use the "security gateway" approach, which entails deployment of appliances with Next-Generation Firewall capabilities deployed as a centralized model, which entails a single box that integrates all necessary security applications.

security and content filtering solution will help prevent unauthorized transmission of EMRs over the network.

Easing deployment and management of EMR security

The addition of EMR security to HIPAA and other compliance initiatives underscores importance of using a strategy that simplifies deployment and management of all security controls. For healthcare organizations, security is not a "core competency," yet as related expectations rise, so do the operational burdens of meeting obligations for compliance. Cost containment through lower capital expenditures and better operational efficiency is essential. For this reason, security solutions for protecting EMRs should be simple to deploy and manage.

Many healthcare organizations have chosen to use the "security gateway" approach, which includes deployment of appliances with Next-Generation Firewall (NGFW). Next-Generation Firewall integrates all necessary security applications, replacing the old model of deploying and managing multiple servers and security applications, and manually integrating operational data for compliance reporting.

NGFWs are deployed at the network edge for comprehensive coverage of threats inside and outside the organization. They are centrally managed with one simple interface. A huge operational benefit to NGFWs stems from built-in integration—it automates the synthesis and monitoring of enterprise security data, which makes fulfillment of reports for security compliance a simple, fast procedure.

With EMRs, the healthcare ecosystem is on the cusp of a major change in how it does business. Protecting EMRs with appropriate security controls is an essential mandated requirement by the federal government. By leveraging existing security controls—especially innovations such as the Next-Generation Firewall, SSL VPNs, email security, and centralized management and reporting—healthcare organizations can rapidly fulfill the new mandate and tap the benefits of medical record automation.

Dell SonicWALL for flexible EMR security

Dell™ SonicWALL™ provides leading appliance-based security solutions for EMR systems. Solutions scale from small- and medium-sized healthcare organizations to the largest institutional providers. Dell SonicWALL includes a full range of security controls to ensure the safety and protection of EMRs.

For more information, visit **www.sonicwall.com/healthcare**.

DELL SonicWALL