SECURITY AND PRIVACY IN HEALTHCARE

White Paper

The New Prescription for Privacy: Understanding and Meeting Security Requirements for Electronic Health Records

Symantec

The New Prescription for Privacy: Understanding and Meeting Security Requirements for Electronic Health Records

Contents

Introduction

Technology continues to make information more readily available to a larger group of people than ever before. Yet even as the latest technological advances bring a greater wealth of opportunities for sharing and distributing knowledge, each advance also increases the risk that sensitive data will land in the wrong hands. The more sensitive the data, the greater the risk—and few industries handle a larger volume of sensitive data than the healthcare industry.

Passed by Congress in February 2009, the American Recovery and Reinvestment Act (ARRA) was designed to jumpstart the nation's economy by boosting investment in the health sector. Key provisions of the legislation included as much as $27 billion to support the adoption of Electronic Health Records (EHRs) among U.S. healthcare providers by 2012, with financial incentives for those who did and penalties for those who did not. One year later, Congress followed up ARRA with the Patient Protection and Affordable Care Act (PPACA), which required healthcare providers to share patient data via information exchanges.

For many healthcare organizations, EHR implementation is now complete. "Meaningful use" is now the challenge at hand. And the simple fact is that a significant number of U.S. health providers remain unprepared for the real privacy and security challenges to come, and healthcare security is among the worst of all industries.[1]

This report looks at the challenges and requirements of protecting confidential patient data online, the risk of security breaches in the world of EHR, and the measures that healthcare organizations must take in order to achieve and maintain compliance.

EHR Adoption: The New Industry Standard

As recently as 2009, 90 percent of U.S. physicians had yet to implement a complete EHR system.[2] Meanwhile, the situation in other countries was the complete reverse: 98 percent of primary-care physicians already used EHRs in the Netherlands, 92 percent in New Zealand, and 89 percent in the United Kingdom.[3]

The United States is no longer so far behind the pack. A 2012 Medscape survey of 21,000 American physicians across 25 specialties found that 82 percent of respondents either currently used or were in the process of implementing an EHR. A mere six percent said they planned to go without.[4]

This meteoric rise in adoption has led to significant—and largely salutary—changes in the EHR marketplace. Competition among vendors has begun to drive down the cost of these systems while expanding their capabilities. As a result, the next generation of EHR systems promises to be more affordable, more interoperable with other systems, and more patient-centered in design.[5] These factors will no doubt eliminate the few remaining objections to EHR implementation, making adoption more or less universal over the next decade.

1. Source: The Washington Post.
2. Source: Centers for Disease Control and Prevention.
3. Source: Modern Healthcare.
4. Source: Medscape.
5. Source: California Healthcare Foundation.

The Meaning of "Meaningful Use"

The ARRA specifies a total of 25 meaningful use objectives for professionals, along with 24 objectives for hospitals and critical access hospitals (CAHs). These objectives address the three main components behind the term "meaningful use":

1. The use of a certified EHR in a meaningful manner, such as e-prescribing.
2. The use of certified EHR technology for the electronic exchange of health information to improve quality of healthcare.
3. The use of certified EHR technology to submit clinical quality and other measures.[6]

Many ARRA objectives focus on the exchange of electronic health information, because the greatest benefits lie in the ability to share data quickly and easily among healthcare providers anywhere in the U.S. These benefits extend far beyond the provider, with considerable advantages for the payer and the patient as well:

- **Continuity from provider to provider.** With EHRs, patients' complete health history moves with them once their provider joins a health information exchange (HIE).

- **Fewer errors in prescriptions.** A provider sends an electronic prescription directly to the pharmacy, and the system generates an alert in the case of any potential adverse drug interactions.

- **Real-time tracking and alerting for more effective, efficient patient care.** New analytical tools continuously track the information a caregiver enters into the EHR, sending alerts when changes occur to inform caregivers that a patient's condition may be on the decline. These same tools track when and why patients are re-admitted, helping hospitals design specific programs to reduce unnecessary return visits.[7]

The Privacy Mandate

The term "meaningful use" would mean very little if it failed to address concerns around privacy and security. For that reason, the strict privacy requirements set down by the Health Insurance Portability and Accountability Act (HIPAA) are embedded quite deeply in the Medicare and Medicaid EHR Incentive Programs.

In order to fulfill the basic requirements for Stage 1 of Meaningful Use, healthcare providers must confirm that they have satisfied 15 "core measures."[8] The last of these measures specifies that providers—including hospitals and CAHs—will take all reasonable precautions to protect electronic health information by conducting, and acting upon, a thorough security risk analysis.[9]

---

6. Source: Centers for Medicare and Medicaid Services.
7. Source: MedCity.
8. Source: Centers for Medicare and Medicaid Services.
9. Source: Ibid.

Beyond the federal requirements, many states have their own privacy statutes as well; one of the most notable is California's AB 1298, which obliges businesses engaged in healthcare to notify residents after any security breach of unencrypted data.[10] Furthermore, failure to properly protect patient data in the state of California can result in considerable penalties—up to $25,000 per patient.[11]

In short, a violation of these federal and state regulations is no mere slap on the wrist. If your organization does not yet have an actionable strategy in place for ensuring the security of patient data, you're not simply behind the curve—you're running a considerable regulatory, legal, and financial risk.

Addressing Patients' Privacy Concerns

Many consumers would probably be inclined to say that the security of their financial data is of greater concern than the privacy of their healthcare records. However, the long-term consequences of healthcare data breaches are generally far more severe. With credit card breaches, most users are held liable for no more than $50; fraudulent transactions can be cleaned up quickly, and new credit card numbers can eliminate the threat of further unapproved charges.

Not so with private healthcare data. Once confidential information is spilled onto the Internet, it can't be put back into the bottle. Friends, coworkers, family members, and potential employers may forever know what was supposed to be a private matter between you and your doctor, leading to embarrassment, job discrimination, and other serious consequences. In cases like these, no amount of money paid to a state or federal regulatory agency can mitigate the potential damage to a patient, or to the reputation of a doctor or hospital. As Ponemon Institute founder Dr. Larry Ponemon explains, "In a trusted industry like healthcare, there's a high expectation of good stewardship of personal information. …You can't just give patients some sort of discount and win them back."[14]

As more consumers become aware of what's at stake, more will begin to demand real evidence that healthcare providers take their privacy seriously. It is perhaps in providers' best interest to address these concerns proactively, assuring consumers in the strongest concrete terms possible that they can conduct healthcare transactions and store personal data online with confidence.

Next Steps Toward Smarter Security

While most healthcare organizations will likely have security solutions in place for data "at rest" (for example, information stored in a database), protection for data "in transit" sometimes receives less attention. In order to protect confidential patient data from unauthorized access, healthcare organizations need a systematic approach to security across the entire online transaction, thus mitigating threats at multiple levels. A multi-layer strategy like this protects EHR transactions at every critical point.

Data Breaches: How Common Are They?

All too common, as it turns out. According to the HHS, nearly 20 million patient records were compromised between 2010 and 2012.[12] The agency counted 380 significant breaches (each affecting 500 or more individuals) in the year 2011 alone.[13]

Privacy Matters, but Quality Care Matters Even More

A recent study shows that a large number of consumers are concerned about the privacy of their health information. The majority of respondents, however, said they were comfortable with physicians sharing their private data electronically, provided that it leads to better care.[15]

10. Source: California Department of Health Care Services.
11. Source: Foley & Lardner LLP.
12. Source: InformationWeek.
13. Source: U.S. Department of Health & Human Services.
14. Source: Ponemon Institute.
15. Source: InformationWeek.

SSL Certificates

Secure Sockets Layer (SSL) certificates are one of the first lines of defense in this multi-layered approach to protection. SSL technology establishes a private communication channel where data can be encrypted during online transmission, protecting sensitive information from electronic eavesdropping. In order to obtain an SSL certificate with a high level of authentication, organizations must prove that they are a legitimate business and that they own the domain name or names that they want to secure. This enables patients to verify the identity of the website owner, thus gaining assurance that the healthcare website is authentic.

Thanks to this authentication process, patients can also be alerted to phishing attacks. In a typical phishing scam, cybercriminals create a site that looks like a "real" site. If patients enter in their social security numbers or other sensitive information, the data will be sent directly to the criminals instead of the EHR system. A fake EHR portal could go unnoticed for months, quietly collecting personal information from hundreds (if not thousands) of unwitting patients.

Different types of SSL certificates offer different levels of encryption and authentication. Although not required by any law or governing agency, Extended Validation SSL Certificates provide the best protection for patients. With EV SSL, many patients will see a green bar in their web browsers when they log into an EHR system, giving them a clear signal that their data is protected. The authentication process for EV SSL is also more rigorous, helping to ensure that only legitimate healthcare providers obtain SSL security.

A vast majority of web users are already familiar with SSL security and see it used on banking web sites and ecommerce sites. In fact, research shows that visible signs of SSL security—including padlock icons, site seals, and the green bar—make visitors feel more comfortable about divulging private information on web sites. For EHRs, SSL security is critical not just for protecting patient data, but also for helping build trust.

Health providers should maintain SSL security at all times on their patient-facing sites, protecting each patient's end-to-end online experience from a wide range of criminal activities, including phishing and side-jacking. In order to provide patients that level of protection, health providers also need to implement an advanced and robust SSL certificate management system that can provide visibility and monitoring of all SSL certificates regardless of issuing Certification Authority from one single console. Additionally, an SSL certificate management system that offers automated installation, renewal, and replacement of certificates would help healthcare organizations to increase operational efficiency and eliminate errors introduced from manual steps.

When It Comes to Security, Focus Is Key

"We need to get people focused on the one simple thing they can do in the security space and move the needle in terms of protecting patient privacy. Encryption is one of those rare focus areas that can make a huge difference."

—Doug Pollack, Chief Strategy Officer, ID Experts[16]

Two-Factor Authentication and Fraud Detection

Two-factor authentication (2FA) requires an individual to use two independent forms of identification to gain access to a website or online portal. In practice, this often means combining regular usernames and passwords chosen by a user with one-time credentials, such as passwords or codes, generated by the

16. Source: InformationWeek.

authentication system and delivered via tokens, cards, mobile phones, or other devices. Because one-time passwords are random, generated automatically, and provided only to the user who is trying to log into a specific site, two-factor authentication can help ensure that only authorized patients and providers have access to a particular EHR system.

While it is possible for IT professionals to create self-signed SSL Certificates and two-factor authentication systems, it would be extremely time consuming and most likely cost-prohibitive, especially for smaller health practices that do not have large IT teams. Turning to an expert third-party provider like Symantec is more cost-effective and guarantees that organizations can take advantage of the most advanced security solutions currently available.

Symantec Provides Complete Website Security for EHR Systems

Given the complexity of EHR technology, the tangle of state and federal regulations that govern EHRs, and the severe consequences that can stem from lax or improper security, effective protection of EHRs may seem like a huge challenge. However, Symantec offers comprehensive solutions that can help healthcare organizations of all sizes secure their patients' private data.

With **Symantec Website Security Solutions,** healthcare organizations can protect any EHR with the most trusted solution for web-based encryption and security. Symantec SSL Certificates are available in a full range of solutions, including Extended Validation so patients can be sure that their confidential medical information is safe. Symantec SSL Certificates also include the Norton™ Secured Seal, which is the most recognized symbol of trust on the Internet. In addition to helping patients see that a site is safe, the certificate also comes with vulnerability assessment and daily website malware scanning to protect EHR portals and build trust with users.

Meanwhile, **Symantec Validation and ID Protection Service (VIP)** offers 2FA technology so that organizations can add an extra layer of security with one-time passwords (OTPs), giving patients even more confidence that their identities are protected.

Conclusion

Implementing EHR technology involves more than just choosing a barebones system and entering a few patients' names. In order to qualify for incentives and avoid penalties, providers must demonstrate "meaningful use" of certified EHR systems. According to government-created objectives and measures, a key part of meaningful use is the ability to share medical information securely between providers and across organizations.

While this may seem like a difficult task, cost-effective, easy-to-use security technologies are available to help healthcare providers protect their EHR systems—and their patients' confidential data. SSL certificates serve as a first line of defense in any multi-layered approach to protection, while 2FA offers an additional layer of security that verifies and protect the identity of EHR users.

No matter how your organization decides to secure its EHR system, working with a trusted third party like Symantec will help ensure that patient records are always protected with the most advanced security solutions currently available. With Symantec, providers can be sure that their EHR systems—and the vital data they contain—are safe, so doctors and hospitals can focus on delivering the best possible care to their patients.

More Information

Visit our website

http://go.symantec.com/ssl-certificates

To speak with a Product Specialist in the U.S.

Call toll-free: 1(866) 893-6565 or 1(650) 426-5112

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1 (866) 893 6565
www.symantec.com