WHITE PAPER

White Paper

A Prescription for Privacy: What You Need to Know About Security Requirements for Electronic Health Records

Now from Symantec™ | VeriSign Authentication Services

VeriSign Trusted™

A Prescription for Privacy: What You Need to Know About Security Requirements for Electronic Health Records

Contents

Introduction

The history of medicine is filled with technological discoveries and innovations that have improved quality of life and enhanced patient care for billions of people around the globe. With a nudge from recent changes in the law, technology is about to revolutionize the healthcare industry once again.

Passed by Congress in 2009, the American Recovery and Reinvestment Act (ARRA) was designed to jumpstart the nation's economy. Given that healthcare makes up one-sixth of the U.S. economy, more than any other industry,[1] it's no surprise that ARRA contains several key provisions aimed at boosting investment in the health sector. These include measures that set aside as much as $27 billion to support the adoption of electronic health records (EHRs) by healthcare providers in the United States. With the passage of ARRA, the push is on to implement EHR systems by 2012, and there are financial incentives for those who do—as well as potential financial penalties for those who don't—comply with the new law.

As organizations implement EHRs—or as they ramp up their existing systems to make them more robust—concerns about patient privacy will move to the forefront. In particular, ARRA contains specific language regarding the "meaningful use" of EHRs, wording that points to an increased emphasis on the sharing of medical information. "Meaningful use" may be a legislative term of art, but many healthcare organizations are currently unprepared for the real privacy and security challenges that it presents.

This report looks at the challenges surrounding the new world of EHR technology, including the requirements that govern protecting confidential patient data online, as well as security breaches and other risks that come with storing and accessing that information with web-based systems. The report also details the measures that organizations need to start taking right now to prepare for the upcoming changes in the healthcare industry.

It's No Longer a Matter of If, but When

Even though ARRA champions the adoption of EHR technology, it's not just legislators who believe these systems can improve healthcare. In fact, recent research shows an overwhelming majority of Americans think that doctors who use a computer system to store their health information instead of paper-based records provide them with better care.[2] Patients' desire for electronic records and the new legislation mean it's no longer a question of *if* EHRs will be adopted on a wide scale, but *when* and *how*.

While EHR systems can indeed improve efficiency and patient outcomes, they represent one of the most drastic upheavals in recent history for individual doctors, group practices, and other related healthcare organizations. For this reason, adoption of EHR technology has been slow. The number of providers using EHRs has been steadily increasing, but the CDC reports that 90 percent of physicians have yet to implement a complete EHR system.[3]

1. http://www.usatoday.com/news/health/2009-06-19-health-economy_N.htm
2. http://www.healthcareitnews.com/news/survey-78-percent-patients-believe-ehrs-boost-care
3. http://www.cdc.gov/nchs/data/hestat/emr_ehr_09/emr_ehr_09.htm

While the majority of providers in the United States have been dragging their feet, healthcare organizations in other countries have raced to adopt EHR technology and are now far ahead of their American counterparts. In the Netherlands, 98 percent of primary-care physicians use EHRs and New Zealand boasts a 92 percent adoption rate. The United Kingdom is a close third with an 89 percent use rate, and Australia is fourth with 79 percent.[4] To close the gap, ARRA lays out generous incentives to encourage providers to make the transition to EHR technology.

The Carrot and the Stick—EHR Incentives and Penalties

Healthcare organizations are under pressure to move to EHR systems sooner rather than later, and the changes are being driven by more than just the desire to improve patient care. A subsection of ARRA called the Health Information Technology for Economic and Clinical Health (HITECH) Act offers federal incentive payments to doctors and hospitals who submit claims to Medicare or treat a caseload base that consists of at least 30 percent Medicaid patients.[5] These eligible providers must adopt EHRs and demonstrate that they are using EHR systems in ways that can improve quality, safety, and effectiveness of care. Payments begin at $44,000 over five years for eligible professionals, while incentives of $2 million in base payments are available for hospitals.

Eleven states have already launched Medicaid EHR incentive programs, and a parallel Medicare program launched in May 2011.[6] Four states—Oklahoma, Kentucky, Louisiana, and Iowa—have issued more than $20 million in incentives so far. These include $2.8 million for the University of Kentucky's teaching hospital, University of Kentucky HealthCare, and $1.3 million for Central Baptist Hospital in Lexington. In Oklahoma, two physicians at the Gastorf Family Clinic of Durant, Oklahoma received incentive payments of $21,250 each for having adopted certified EHR systems.[7]

Medicare EHR Incentives for Eligible Providers

Calendar Year	First Year of Participation				
	2011	2012	2013	2014	2015+
2011	$18,000	---	---	---	---
2012	$12,000	$18,000	---	---	---
2013	$8,000	$12,000	$15,000	---	---
2014	$4,000	$8,000	$12,000	$12,000	---
2015	$2,000	$4,000	$8,000	$8,000	$0
2016	---	$2,000	$4,000	$4,000	$0
TOTAL	**$44,000**	**$44,000**	**$39,000**	**$24,000**	**$0**

Medicare Penalties for Eligible Providers

Reductions in Medicare Fee Schedule for Non-Compliance	Starting in 2015	2016	2017	2018	Ongoing
-1%	$3,000				
-2%		$6,000			
-3%			$9,000		
-4%				$12,000	
-5%					$15,000

Medicaid EHR Incentive Payment Schedule for Eligible Providers Qualifying in 2011

Calendar Year	Payment
2011	$21,250
2012	$8,500
2013	$8,500
2014	$8,500
2015	$8,500
2016	$8,500
TOTAL INCENTIVE	**$63,750**

For example, a provider qualifying for the Medicaid EHR Incentive in 2011 would receive a total incentive of $63,750 paid out over six years. Providers can also qualify in 2012 or later, with the last possible year to qualify being 2016. No matter when the provider qualifies between 2011 and 2016, the payments are still spread out over a six-year period.

It is clear that HITECH Act incentives are available to a wide variety of private and public healthcare organizations, but the timeframe to register for the funds is not open-ended. All providers must begin participation by 2012 to receive the maximum payments.[8]

4. http://www.modernhealthcare.com/article/20090206/REG/302069989
5. http://uwf.edu/sahls/medicalinformatics/docfiles/Physicans_Guide_to_EHR_Reimbursement.pdf
6. http://www.informationweek.com/news/healthcare/EMR/showArticle.jhtml?articleID=229219415
7. Ibid.
8. https://www.cms.gov/ehrincentiveprograms/

While there are strong financial incentives to encourage healthcare organizations to adopt EHR technology, the HITECH Act also outlines penalties for eligible providers that do not move to these systems. Some details are still being decided, but doctors who submit claims to Medicare and do not implement EHRs by 2015 will see reductions in their Medicare fee schedule, starting with a one percent reduction in 2015, two percent in 2016, three percent in 2017, and beyond.[9]

First Step: Implementing a Qualified EHR System

To comply with the provisions of ARRA and receive incentive payments—not to mention to avoid being penalized—healthcare organizations must implement "qualified" EHR systems, but what does qualified mean? As defined in the bill, a qualified EHR system "includes patient demographic and clinical health information, such as medical history and problem lists; and has the capacity to

(i) provide clinical decision support;
(ii) support physician order entry;
(iii) capture and query information relevant to health care quality; and
(iv) exchange electronic health information with, and integrate such information from other sources."

Government agencies have taken the guesswork out of finding qualified EHR systems by providing lists of vendors. The Centers for Medicare and Medicaid Services (CMS) has compiled a list of qualified EHR vendors that are appropriate for any doctor or hospital that receives Medicare or Medicaid funds, while the Office of the National Coordinator for Health Information Technology (ONC) maintains a list of EHRs and EHR modules that have been certified by an ONC-Authorized Testing and Certification Body.

Aside from the financial impact of implementing an EHR system—something that the drafters of ARRA hope to mitigate with incentives—one of the most pressing concerns for large and small practices alike is how to integrate EHRs into their existing workflows and demonstrate that they are using the new systems effectively. In fact, information sharing is a key part of the "meaningful use" objectives defined by an advisory committee to the U.S. Department of Health and Human Services. Clearly, as the critical mass of organizations moving to EHRs grows, the need to share this data electronically will grow too.

Sharing Information to Achieve "Meaningful Use" of EHR Technology

Even if healthcare organizations select a qualified, certified EHR technology and implement it, they still need to demonstrate "meaningful use" of the system to receive incentive payments. The exact definition of the term is in flux, but ARRA specifies three main components of 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 electronic exchange of health information to improve quality of health care
3. The use of certified EHR technology to submit clinical quality and other measures[10]

9. http://www.ama-assn.org/ama1/pub/upload/mm/399/arra-hit-provisions.pdf
10. https://www.cms.gov/EHRIncentivePrograms/30_Meaningful_Use.asp

There are a total of 25 meaningful use objectives for professionals and 24 objectives for hospitals and critical access hospitals (CAHs).[11] Many of these objectives focus on the exchange of electronic health information, and it's easy to see why. The ability to share data quickly and easily across all of the various providers involved in modern patient care is one of the greatest benefits that EHR technology offers.

The objectives also set out requirements that advocate giving patients access to their personal electronic medical information. When healthcare organizations enable patients to retrieve or send their confidential data online, securing that information becomes a critical part of the equation. For all intents and purposes, providers cannot achieve meaningful use without sharing patient data, and confidential medical information cannot be shared without making sure that the data is protected from hackers, cybercriminals, and other malicious online threats.

"I am seeing organizations shift their focus from implementation of electronic health records to a focus on the next phase of meaningful use, specifically how they are going to share patient records though health information exchanges."

– Rick Kam, president and co-founder of ID Experts, a provider of data breach solutions.[12]

Security Becomes a Critical Issue

As more and more doctors and hospitals weigh the risks and rewards of implementing EHR systems, security lapses—and the danger that private health information may become publically exposed—is top of mind for the entire healthcare industry. According to Larry Walker, president of a governance consulting company that works with healthcare organizations, "Patient health information data breaches are one of the most significant legal and public trust risks facing hospital governing boards, which are legally and ethically accountable for the results of a breach. The board of trustees has a fundamental fiduciary responsibility to ensure that patients' health information is safe and secure at all times."[13]

In addition to the meaningful use objectives outlined by ARRA, the Centers for Medicare and Medicaid Services has developed a series of measures detailing the procedures and functions that EHR technology must support. Security is so essential to EHRs that CMS has created a measure that focuses specifically on protecting electronic health information. This particular directive, Measure 15, states that eligible professionals must "protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities."[14] A similar measure is also in place for hospitals and CAHs.

Beyond these guidelines and directives, there are additional laws and regulatory requirements that must be taken into consideration, including the Health Insurance Portability and Accountability Act (HIPAA). While HIPAA addresses the privacy of electronic health care transactions, the HITECH Act clarifies these rules, outlines stiffer civil and criminal penalties, and strengthens enforcement against healthcare organizations that fail to protect EHRs.[15]

The HITECH Act enhancements to HIPAA also require healthcare organizations to notify patients if a data breach occurs. Not only that, but the HITECH Act extends

11. Ibid.
12. http://www.healthcareitnews.com/news/top-7-trends-health-information-privacy-2011
13. Ibid.
14. http://www.cms.gov/EHRIncentivePrograms/Downloads/15ProtectElectronicHealthInformation.pdf
15. http://www.healthleadersmedia.com/content/HEP-228444/Economic-stimulus-act-heightens-HIPAA-enforcement.html

these privacy requirements to business associates (such as EHR vendors) that work with HIPAA-covered entities.[16]

Even if providers are in compliance with federal law, they still have to worry about state laws and regulations. Some states, such as California and Connecticut, have passed measures that are even stronger than HIPAA and the HITECH Act, including California's healthcare data breach law AB 1298.

The financial penalties for violating these and similar laws can be severe. For example, the California Health and Safety Code 1280.15(a) requires health facilities to properly protect patient data. Violations of this requirement can result in fines of up to $25,000 per patient and up to $17,500 per subsequent occurrence of unlawful or unauthorized access, use, or disclosure of patients' medical information.[17] These fines can add up quickly, as this example shows: Between March and November 2010, the California Department of Public Health fined 12 health facilities about $1.5 million as a result of data breaches.[18] With the HITECH Act enhancements, providers that violate HIPAA's privacy standards face fines anywhere from $100 to $50,000 per incident depending on whether the breach could have been reasonably avoided.[19]

Given the stiff consequences, healthcare organizations of all sizes must take appropriate steps to secure the patient data stored in their EHR systems. This involves not only putting the proper technology in place to safeguard medical information, but helping patients understand that personal details contained in their health records are being protected.

Reassuring Patients That Their Information is Safe

Even though many people believe that computer-based records help doctors and hospitals provider better care, consumers still need assurance that it's safe to conduct healthcare transactions and store their healthcare information online. In fact, a recent study showed that almost half of 1,000 people surveyed after a visit to a healthcare facility believed that EHRs will have a negative impact on the privacy of their personal health information.[20]

It turns out patients have good reasons for being concerned. According to a report by the Ponemon Institute, 58 percent of healthcare organizations have little or no confidence in their ability to secure patient records appropriately, and 69 percent said they had inadequate policies or procedures in place to safeguard medical records. Moreover, 70 percent of hospitals stated that protecting patient data is not a top priority. These percentages roll up into one startling fact—data breaches cost the healthcare industry $6 billion annually.[21]

Healthcare Data Security by the Numbers

- 58% of healthcare organizations have little or no confidence in their ability to secure patient records appropriately
- 69% of providers have inadequate policies or procedures in place to safeguard medical records
- 70% of hospitals do not believe protecting patient data is a top priority

Source: Ponemon Institute

16. http://www.itbusinessedge.com/cm/blogs/bentley/hitech-act-means-more-aggressive-hipaa-enforcement/?cs=31212
17. Ibid.
18. http://www.informationweek.com/blog/main/archives/2010/12/california_does.html
19. http://www.healthleadersmedia.com/content/HEP-228444/Economic-stimulus-act-heightens-HIPAA-enforcement.html
20. http://www.informationweek.com/news/healthcare/security-privacy/showArticle.jhtml?articleID=229300722
21. http://www2.idexpertscorp.com/resources/healthcare/healthcare-articles-whitepapers/ponemon-benchmark-study-on-patient-data-security-practices/?utm_source=Ponemon%2BRedirect&utm_medium=Online&utm_campaign=Ponemon%2BRedirect/

For patients, data breaches often come with a different type of price tag that exacts payment measured in loss of confidence, not dollars. When a credit card breach occurs and thieves use stolen numbers to make purchases, most users are held liable for $50—if that—and fraudulent transactions can be cleaned up fairly quickly and easily. This is not always the case with private health information.

If confidential medical data is leaked and made public, it may be next to impossible to erase. Anyone with an Internet connection—including friends, family, co-workers, and employers—may have instant access to highly personal information, 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."[22]

Patients are worried about the safety of their data and providers are concerned about their ability to protect it. The stakes are high for patients and providers alike, so any potential security vacuum in EHR technology must be addressed proactively.

What Healthcare Organizations Need to Know About Security

While most organizations will likely have security solutions in place for data that is "at rest" (for example, information that is stored in a database), protection for data that is "in transit" or being transmitted across the Internet often gets less attention. To protect confidential patient data from accidental or malicious unauthorized access, healthcare organizations need a systematic approach to security across the entire online records transaction that mitigates threats at multiple levels. A multi-layer strategy like this protects EHR transactions at each critical point, from authenticating the EHR web site and securing data transmission, to protecting the identities of patients and other EHR users.

SSL Certificates

One of the first lines of defense in this type of layered protection is SSL security. Secure Sockets Layer—commonly abbreviated 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 own the domain name or names that they want to secure. This enables patients to verify the identity of the web site owner and ensure that the healthcare organization that operates it is indeed authentic. Healthcare organizations should avoid domain-validated SSL Certificates as these offer far lower levels of authentication.

22. http://www.fiercehealthcare.com/story/data-breaches-cost-your-hospital-1-million-year/2010-11-10

The verification process that SSL security requires can also alert patients to serious online threats like phishing attacks. In a typical phishing scam, cybercriminals will create a site that looks almost exactly like a "real" site, or in this case a "real" EHR portal or interface. If patients enter in their social security numbers or other sensitive information into a phished EHR site, the data will be sent directly to the criminals instead of healthcare professionals. A fake EHR portal could go unnoticed for months, quietly collecting personal information from hundreds if not thousands of unwitting patients.

There are several different types of SSL Certificates that offer different levels of encryption and authentication. Although not required by any law or governing agency, Extended Validation (EV) SSL Certificates provide the best protection for patients. With EV SSL, most 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 and regulated, helping to ensure that only legitimate healthcare providers obtain this level of SSL security.

The vast majority of web users are already familiar with SSL security and see it used on numerous banking web sites and ecommerce sites. In fact, research shows that visible signs of SSL security—including padlock icons, site seals, and the green EV bar—make visitors feel more comfortable about divulging private information on web sites.[23] For EHRs, SSL security is critical not just for protecting private medical data, but also for helping build trust with patients so they feel comfortable obtaining healthcare services from providers who use these systems.

SSL Certificates act as a vital layer of security, but they are not the only one. By adding two-factor authentication, healthcare organizations can make their EHR security even more comprehensive and robust.

Two-Factor Authentication

Two-factor authentication, also called 2FA or strong authentication, is a system that requires an individual to use two independent forms of identification to gain access to a web site 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 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.

---

23. http://www.aberdeen.com/Aberdeen-Library/7044/RA-secure-sockets-layer.aspx

Symantec Provides Complete 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, protecting EHRs effectively may seem like a huge challenge. However, VeriSign® Authentication Services, now from Symantec, offers a comprehensive suite of products and services that can help healthcare organizations of all sizes secure their EHRs. These solutions include:

VeriSign SSL Certificates – Protect any EHR with the most trusted solution for web-based encryption and security. VeriSign 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. VeriSign SSL Certificates also include the VeriSign 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 a daily web site malware scan and other features to protect EHR portals and build trust with users.

VeriSign Identity Protection Authentication Service – With two-factor authentication from VeriSign, organizations can add an extra layer of security with one-time passwords, giving end users even more confidence that their identities are protected.

Conclusion

Spurred on by the recent passage of the American Recovery and Reinvestment Act (ARRA), more doctors and hospitals are moving to electronic records systems and exploring ways to more fully implement them within their practices. To encourage more providers to use EHR technology, ARRA outlines significant monetary incentives (as well as serious penalties) intended to lessen the financial burden while enabling providers to make the transition faster.

As many healthcare organizations are discovering, implementing EHR technology involves more than just picking a bare bones system and entering in a few names. In order to qualify for incentives and avoid penalties, providers must also show “meaningful use” of certified EHR systems. According to government-created objectives and measures, a key part of meaningful use is sharing medical information between providers and across organizations.

Even though many people believe that EHRs will help their doctors improve patient care, they still need to be reassured that their private medical data is safe. Beyond building confidence with patients, state and federal laws also mandate that providers safeguard confidential information and prevent data breaches.

While this may seem like a difficult task, there are several cost-effective, easy-to-use security technologies that healthcare providers of any size can use to protect their EHR systems. SSL Certificates encrypt medical data during online transmission and make patients aware of potential phishing attacks, while two-factor authentication offers an additional layer of security that verifies and protects the identity of EHR users.

No matter how an 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.

For more information about how Symantec can help your organization protect EHRs, go to www.verisign.com.

More information

Visit our website

http://www.verisign.com

To speak with a Product Specialist

Call 1 (866) 893-6565 or 1 (650) 426-5112, option 3

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. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1 (800) 721 3934
www.symantec.com

Now from Symantec™ | VeriSign Authentication Services

VeriSign Trusted™