WHITE PAPER:
NEW WORLD ORDER: EFFECTIVELY SECURING
HEALTHCARE DATA THROUGH SECURE

NEW WORLD ORDER: EFFECTIVELY SECURING HEALTHCARE DATA THROUGH SECURE INFORMATION EXCHANGES

Who should read this paper

Individuals focused on the Secure Sharing of Public Health Information including Federal, State, and Local Government CIOs, CMOs, CISOs

Confidence in a connected world. Symantec.

Content

Why SIE, Why Now? 1

What is a Health Information Exchange (HIE)? 2

Protecting the Protected 2

The Structure of an SIE: Identification, Control, Protection and Discovery 4

Conclusion: What's Next for SIE? 6

Why SIE, Why Now?

An "Unprecedented Opportunity," Fraught With Risks

"Health care professionals and hospitals are taking advantage of this unprecedented opportunity to begin using smarter, new technology that improves care and creates the jobs we need for an economy built to last."

Kathleen Sebelius

Secretary

U.S. Department of Health and Human Services

Healthcare, perhaps more so than any other industry, is dominated by the need for the sharing of detailed information. It is also an industry that is overwhelmingly preoccupied with concerns for security and patient privacy. The juxtaposition of these factors is striking: on the one hand, hospitals, physicians, nurses, government agencies, insurance companies and others need to freely obtain and distribute patient information; on the other, that information must be protected and kept confidential, or serious repercussions may ensue. It is, perhaps, one of the most challenging situations created for any industry as a result of today's information age, impacting virtually all healthcare organizations and spanning state, local and federal boundaries.

That challenge has grown significantly with the move from paper records to electronic health records (EHRs) – a move propelled by the federal government's commitment to eliminating paper and making records more easily accessible. Whereas before physicians and other care providers would rely on written charts to document patient information – a process that created its own set of issues – most doctors and organizations are now relying on EHRs, which provide the opportunity for more accurate, easily sharable details. The adoption of EHRs is being driven by the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was designed to bolster the use of EHRs and complementary technology. That approach has worked, and EHRs are now widely accepted as the de facto standard, the driving force for the easy sharing of information among healthcare organizations and the backbone of healthcare technology efforts within state, local, and federal governments.

This massive jump in adoption is hardly surprising, given the number of incentives that have been put into place over the past several years to spur the sharing of health information, not to mention the unique needs of government agencies. Things like the American Recovery and Reinvestment Act of 2009 and various Medicare and Medicaid incentives - although, at this point, mostly exhausted – successfully laid the groundwork for healthcare institutions' investments in technology. Of course, the benefits of doing so have also gone far beyond the financial; organizations and agencies have found that technology has enabled better care coordination, easier access to patient information, expedited claim payment, better assessment of benefit eligibility, improved quality of information (with fewer errors), more productive consumer and patient engagement, and improved efficiency across the board.

All of this openness – enhancing patient care, communication between agencies and providers, and overall productivity – is wonderful. Thus, it's no surprise that Health Information Exchanges (HIEs) – the mobilization of electronic health information across disparate health information systems -- have gained significant traction over the past few years, as reliance upon EHRs has increased. In fact, at the state level, KLAS, an organization that seeks to improve healthcare technology delivery, reported that during 2010 – in the wake of the institution of the HITECH Act – the number of operating public HIEs increased 81% from 37 to 67, while the number of operating private HIEs increased 210%, from 52 to 160.[1]

And yet, openness has its price -- making patient data increasingly vulnerable. This is where the employment of Secure Information Exchanges (SIEs) becomes absolutely critical. SIEs offer a secure way to transfer and access sensitive information, including patients' health records and other personal data. This is, of course, of paramount importance within healthcare, where even inadvertent violations of things like the Health Insurance Portability and Accountability Act (HIPAA) can result in millions of dollars in fines – and worse.

The bottom line is that none of the benefits offered by the electronic sharing of information matter if the information that is being compiled and distributed is not secure. The challenge for healthcare organizations and federal, state and local agencies here is significant, requiring a great deal of planning, diligence, trust-building, and, above all, an unwavering commitment to data protection.

What is a Health Information Exchange (HIE)?

The driving force behind patient care is not just a doctor – it is data that can easily be shared between healthcare organizations, physicians, insurance companies, and others. This data must be able to be distributed and retrieved quickly and easily, regardless of the potential disparity between health information systems. Immediate access to this data can enhance patient care, making treatment more accurate, timely and effective.

This is where the concept of a Health Information Exchange (HIE) comes into play. HIEs provide the ability to move patient information electronically from one network to another, regardless of the differences among various information technology systems. While doing so, HIEs maintain the integrity and "meaning" of the data, regardless of the system it's being accessed on, so that anyone with authorization can view a patient's information without impediment. For example, a physician at a family practice will easily be able to access a patient's hospital records via computer even though the hospital may be on a different network. And they can do so with only a few keystrokes.

HIEs have gained popularity over the past few years, particularly in light of the adoption of Electronic Health Records (EHRs) and federal mandates such as the HITECH Act. This popularity will likely continue to increase as HIEs continue to be backed by federal and state governments which are heavily invested in the concept of secure electronic transfer of patient information.

Better access to patient data, leading to better treatment, is a concept the healthcare industry has long strived for. HIEs are making this a reality.

Protecting the Protected

When it comes to patient records, healthcare organizations have long been cognizant of the need for privacy, security and confidentiality. That awareness, however, has spiked in recent years as the turn toward EHRs became more prevalent. Still, these organizations are facing numerous challenges and impediments in the ongoing battle to ensure that the information contained within EHRs is protected. These challenges range from the mundane to the more technologically advanced, but most revolve around technology. The Centers for Medicare and Medicaid Services (CMS) reports that devices housing important data still present the biggest threats. According to CMS, stolen or lost laptops, USB memory sticks, hard disk drives, and DVDs with unencrypted personal information are particularly vulnerable to data breaches. And that's just as a result of direct human contact, not accounting for the potential for cyber attacks.

As modernization projects surrounding healthcare information continue to grow, so do concerns about data being compromised, particularly as this data is transferred from government agency to provider (and vice-versa). State and local government agencies, for example, are enacting state-regulated and standardized Health Insurance Exchanges (HIXs) which are designed to make it easier for individuals to compare and purchase insurance coverage that's eligible for government subsidies. Of course, HIXs rely on accurate, trustworthy data being

[1] Health Information Exchanges: Rapid Growth in an Evolving Market, June 2011

transferred from providers to agencies and patients. Naturally, this has spurred concerns about fraud and hacking. That is one of the reasons why states are investing significantly – billions of dollars, in many cases[2] – in things like Medicaid fraud control units. HIX is an example of the lofty heights that modernization of patient care is reaching for, but it also exemplifies the intensity of the concerns among state and local governments as more and more data moves electronically.

Beyond the investment in fraud control management, there are additional safeguards like the HITECH Act which adds force to already staunch HIPAA security rules and makes even accidental breaches of electronic health records a costly affair, both literally and figuratively. Financially, breaches can cost organizations millions of dollars. But the damage to public perception can be even more costly and far-reaching. According to HHS.gov, under HITECH, any organization that suffers a breach must notify the individuals impacted "promptly" – generally regarded as no longer than 60 days following the breach. Further, any security breach that involves an individual's personal information is always highly publicized, but when it comes to healthcare records – truly the *most* personal type of information – it can be disastrous for the organization and take years to build back public confidence and trust.

But how is that trust built in the first place? Through standards and safeguards that ensure that the only ones who can access patient records are ones who are authorized to do so. This is where several initiatives come into play.

One, an open source effort known as The Direct Project, is a pilot project started by several companies with the blessing of The Office of the National Coordinator for Health Information Technology. The Direct Project promises a more simplified, streamlined approach to the protection of patient data by offering a simple, scalable, standards-based method for sending encrypted health information over the Internet. As a result, many organizations and agencies have begun to forgo the perceived red tape (including potential political and legal issues) presented by HIEs and adopt standards put forth by The Direct Project.

In addition, The National Institute of Standards and Technology's Electronic Authentication Guideline (also known as NIST 800-63-1) and the United States Office of Management and Budget's E-Authentication Guidance for Federal Agencies (or, OMBD 04-04) both strive to provide federal agencies with guidance for authenticating the identities of individuals attempting to access private data. While not specific to health records, the guidelines, which were first implemented several years ago as the government commenced an effort to reduce paper and make records more easily accessible to citizens, cover virtually every aspect of the dissemination of personal information from a federal government standpoint. These guidelines were developed to maintain the integrity of information never meant for the masses.

There is also the Health Information Trust Alliance (HITRUST), a for-profit, collaborative effort between healthcare, business, technology and information security leaders, all of which have come together to develop the Common Security Framework (CSF). According to HITRUST, CSF is "a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information."[3] Although not a standard, it is designed to ensure that organizations are working harmoniously with various federal programs, including HIPAA and others.

At the end of the day, the protection of health data is not anything fundamentally new. What *is* new is the need for an equal evolution within healthcare of new privacy and security tools. These tools should be designed to allow this environment to adapt to the ever-changing threats that came with the introduction of the electronic system and apply commensurate controls through Compliance, Privacy & Security.

2- http://www.namfcu.net/publications/annual-state-surveys/Statistics%202011%20-%20expanded.pdf
3- http://hitrustalliance.net/about/

Protecting Data, At Rest and in Motion, Through Encryption

Still, securing information gateways is only the starting point for SIEs. The data itself must also be protected, while at rest and in motion. In short, it must be encrypted.

Currently, the HITECH Act requires a federal breach notification for any data that is compromised and has not been de-identified – in short, data that still contains personally identifiable information for an individual. Such a notification can create, at minimum, a public relations nightmare. Prior to HITECH, an amazingly small number of organizations had encrypted healthcare data; that number has since risen significantly, but many institutions are still lacking. The bottom line, however, is simple enough: **encrypted or de-identified data provides a safe harbor from breach notifications, as it is considered secure.** That alone should be incentive enough for organizations to put their best foot forward with regards to EHR encryption.

Open Standards Build the Framework for Effective SIE

While states and federal governments do have standards and guidelines for access to data (through NIST 800-63-1 and OMBD 04-04), there is, unfortunately, no single model for the *exchange* of that data. Therefore, organizations that implement an SIE program must do so in compliance with open standards, such as those provided by the HITECH Act, HIPAA, NIST, and others.

Additionally, a solid SIE solution would do well to mimic the outline put forth by CMS which emphasizes a commitment to:

- Data protection and availability
- High availability/disaster recovery
- Data encryption
- Data loss prevention
- Back-up
- Identity management

By addressing these topics, SIEs can protect an individual's data throughout its entire lifecycle, from creation to storage to access and dissemination.

The Structure of an SIE: Identification, Control, Protection and Discovery

But these are just the foundation of a SIE. The entire structure rests upon several other facets that lead to the control and protection of EHRs through various means.

Chief among these is the aforementioned **user authentication method** which employs back-end identity verification procedures to ensure that whoever is accessing data has authorization to do so. Ideally, this back-end process is coupled with a front-end fraud detection component that monitors and provides warning signs for potentially fraudulent activity. In fact, front-end fraud detection is an extremely important aspect of data protection, but one that is, unfortunately, overlooked by far too many agencies. Using a combination of front- and back-end processes – pairing user authentication with active monitoring – creates a "360-degree" method of security that offers solid protection that makes it extremely difficult for unauthorized parties to gain access to EHRs.

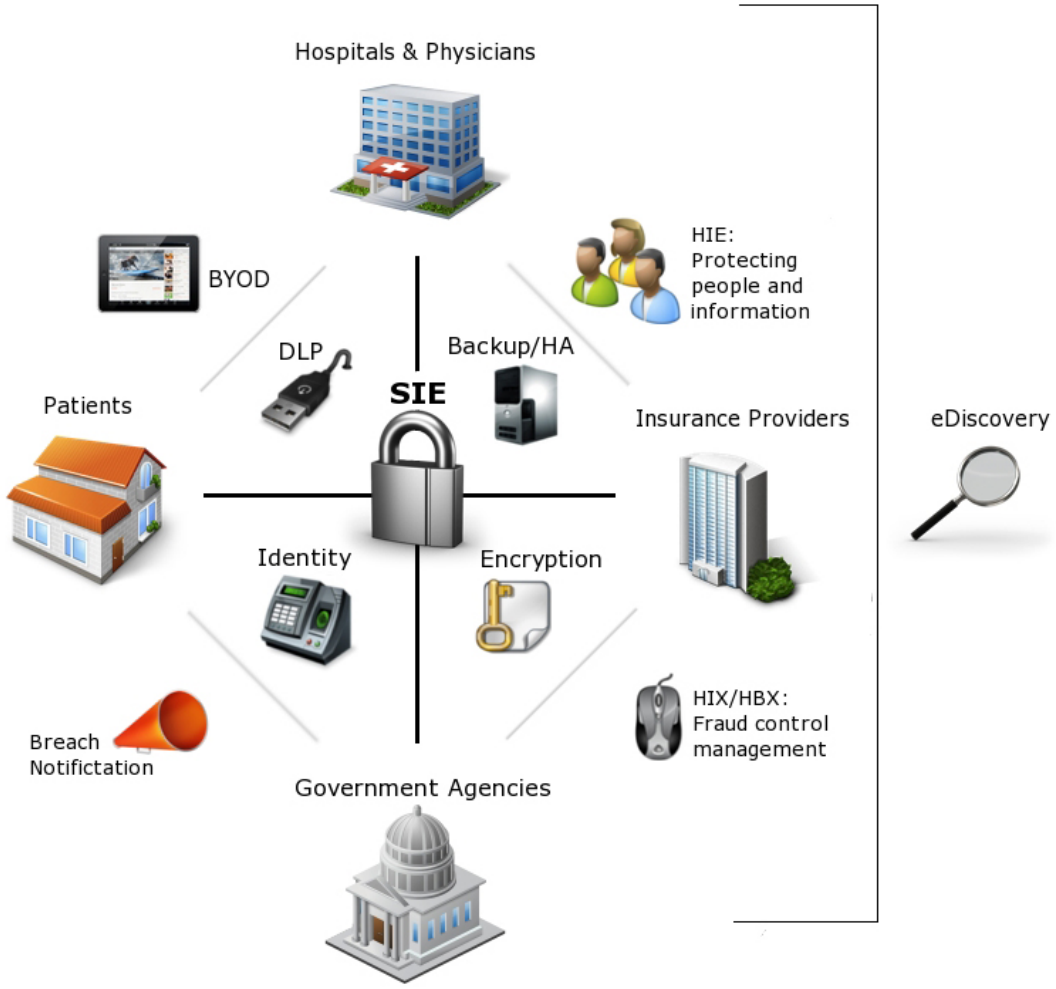
Government organizations and healthcare providers, used to dealing with sensitive data, will also recognize the need for maintaining a **single point of control**. This is particularly important as more and more information moves into the cloud which can mean data spread over multiple environments and locations. Having several different control points is not only a logistical nightmare, but also a threat to the

security of the information. Putting in place a cloud-based Data Loss Prevention (DLP) program is a much more effective approach. DLP can identify specific bits of information that need to be protected – and then secure that information. But even that's not enough. As previously stated, organizations should go a step further to ensure that the data stored in the cloud is encrypted. After all, today's data-disbursed world requires a commitment to as failsafe an approach as possible; this is about as close as one can get.

Of course, there is always the danger that even the most secure data will be subject to malware or virus attacks. Therefore, it's imperative that some form of **Integrated Healthcare Sharing Protection** – such as antivirus monitoring – be put in place. This can provide preventative intelligence that can thwart phishing, malware, and other potentially dangerous attacks that can cause a breach.

Despite the best laid plans in the world, as we know, breaches can and still happen. That is why the final piece of any SIE program should also include an **eDiscovery** component. In the event of a breach, eDiscovery auditing provides both IT and legal professionals with efficient yet thorough classification and retrieval of pertinent information. eDiscovery solutions also maintain audit trails that log when a user accesses data, how long was spent accessing that data, and whether any violations occurred. This type of information gathering is critical in the event of a data breach or fraud investigation – especially when deadlines are tight, and resources tighter.

SIEs and the Public Healthcare Ecosystem



Conclusion: What's Next for SIE?

As always, technology is changing the way information is being recorded, stored and shared within healthcare organizations. The difference today is that most of this information is no longer stored in large data centers. It's stored on smartphones, tablets, and other personal computing devices. It's stored virtually in the cloud. In short, it's everywhere.

The trend known as the "consumerization of information technology" – also known as "bring your own device," or BYOD – is and will continue to heavily impact the way physicians and others interact with patient data. It's no secret that doctors love their iPhone®, iPad®, and other mobile devices; these devices allow them to easily access information wherever they may be. In fact, a recent report by CompTIA indicated that more than 50% of physicians currently use smartphones for work-related purposes.[4] That number will undoubtedly grow, making support for individual mobile devices a key factor in the long-term effectiveness and sustainability of SIEs.

Another trend that will continue to impact the approach to SIEs is healthcare organizations' ever-growing need to store vast amounts of patient data. "Big data" is having a significant effect on many organizations, from hospitals and Medicaid systems that have up to 2 petabytes of spinning disk storage to locations that are dealing with massive amounts of disjointed data. This problem – seemingly insurmountable now – will become increasingly problematic as the amount of patient data continues to pour in. As one healthcare CIO put it, "We are data rich and information poor."

Of course, the drive for the creation of standardized systems centered on the electronic exchange of information will continue unabated. Federal, state and local agencies will continue to adjust to new paradigms set forth by electronic programs designed to ensure that providers are in compliance with federal and state-mandated guidelines and regulations. And while these programs will, ultimately, make information exchange more efficient, there will likely always be concerns about the security of patient data.

Speaking of which, it's a fact that roughly 50% of CIOs across various industries do not trust the data that exists on their own systems. This is, in itself, a problem. After all, SIEs are only as accurate as the data they are designed to protect. If that data is somehow incorrect (at best) or already corrupted (at worst), then even purveyors of the best SIEs in the world have already lost the battle.

Providing Structure to Disorder, Rationality to Chaos

While each of these challenges might seem daunting, there is an effective means of combatting them through SIEs. It involves turning to specifically laid-out approaches designed to provide structure to disorder, rationality to chaos.

We outlined the guidelines and open standards that have been put in place by various government institutions and industry consortiums, including potentially revolutionary initiatives like The Direct Program and HITRUST. These exist for a reason, and can provide any organization with plans for SIEs with solid pathways towards what should be done to ensure that data is kept safe and private. Organizations should work hard to ensure that their SIE efforts comply with the standards laid out by HITECH, HIPAA, NIST and others, and follow the principals outlined by CMS. The components they include are guideposts that can make a vital difference between the ability to protect EHRs, and the potential for it to be compromised.

At the end of the day, healthcare organizations and government agencies share something in common: they want to protect patients. That doesn't just apply to patients' well-being, but personal information, as well. Part of providing the best possible care involves not only treatment, but careful stewardship of medical records and Personal Health Information – not an easy task when such information can be

[4] Third Annual Healthcare IT Insights and Opportunities, CompTIA, November 2011

easily accessed and shared. But it's an important one that requires close attention to security in order to be effective. Implementing a SIE now will help these organizations save both themselves and their patients down the road.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

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

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
10/2012