SOPHOS

Security made simple.

Sophos SafeGuard

Making a case for Encryption in Healthcare

Clinicians and other healthcare professionals don't want to be encumbered by security processes that detract from the time they spend with patients. Yet SafeGuarding protected health information is a provider's responsibility; unfortunately, more than 81 percent of providers and payers acknowledged their organization was attacked within the past two years.[1] A weak state of security jeopardizes patients' physical and digital security, but healthcare organizations can protect patients, employees, and partners without onerous, time-consuming layers of security.

The need for more security comes at a time when healthcare professionals increasingly rely on more digital data flowing from cloud, mobile, sensors, and other computerized devices.

[1] Source: August 2015 KPMG Healthcare Cybersecurity Survey

"ABI Research noted a rise in medical identity theft and fraud following hundreds of cases of personal data breaches over the past two years, the researcher said. "Hospitals, clinics, trusts, and insurers are constantly under attack from malicious online agents. The convergence to digital, the implementation of secure cloud solutions, and the protection of data as it flows through mobile health applications are new security issues the healthcare sector is looking to address."

Healing the Security Sickness

Fortunately, there is strong security medicine that SafeGuards healthcare organizations with minimal side effects in terms of onerous additional processes or laborious steps. Healthcare organizations' CIO, CSO, IT manager, office manager, or physician can easily reduce the risk of data loss by implementing encryption or data security.

"Encryption is one of the most powerful tools available to security professionals seeking to protect sensitive information from unauthorized disclosure. It is the driving force behind the security of networks, web applications, messaging, mobile devices, and many other critical technologies," according to Certification Magazine.

Encryption also plays a key role in healthcare organizations' ability to comply with HIPAA (the Health Insurance Portability and Accountability Act). Although the federal government has not yet mandated encryption (a step some pundits predict), providers must document their d¬¬ecision not to implement encryption and deliver an acceptable alternative, HealthITSecurity.com wrote.

Leading developers like Sophos combine simplicity and security in solutions such as Sophos SafeGuard line of encryption solutions, empowering all organizations — from solo practitioners to the largest hospital chains — to protect themselves. The federal government encourages all healthcare providers to adopt encryption as part of their security practice.

"Our message to these organizations is simple: Encryption is your best defense against these incidents," said Susan McAndrews, deputy director of health information privacy at the Office of Civil Rights, on HHS.gov.

Choosing an Encryption Solution

There are several other criteria healthcare providers should keep top-of-mind when reviewing an encryption solution.

- **Usability:** Encryption must be comprehensive yet simple, so it never affects patient care.
- **Multi-Platform:** You want one encryption solution that works across all devices, regardless of whether healthcare users prefer Apple iOS or Google Android, Windows or Mac.

On the black market, personal health information is far more valuable than credit card data, for example. Health records are worth from a few dollars to **$363 per patient.**[2]

"More than **81 percent** of providers and payers acknowledged their organization was attacked in the past two years."[3]

[2] Ponemon Institute, 2015

[3] Source: August 2015 KPMG Healthcare Cybersecurity Survey

- **Securely and Easily Share Files:** Allows authorized users to safely and simply share encrypted files (while SafeGuarding Protected Health Information or PHI). Data needs to be available quickly and easily among authorized users — while it's also protected from unauthorized users.
- **Adaptable:** Rather than forcing your workflow to change, your encryption software should easily nestle into your day-to-day operations.
- **Industry Respected:** Independent reviews, by both users and third-party testing sites, are a great way to discover what people really think about a solution. Also review healthcare case studies to see how other providers have used the software.
- **Scalability:** Your software should expand to meet your growing needs, and be able to meet the requirements of small, midsize, and large healthcare institutions — with a support staff on hand to respond to your questions 24x7.
- **Proof of Compliance:** In a worst-case scenario, you need a software partner that's able to prove it meets healthcare encryption regulation mandates.
- **Comprehensive:** Your encryption software should be best of breed and part of a suite of security solutions you can implement, either a la carte or as a complete protection package.

The Sophos Solution

With more than three decades' experience, Sophos is expert in protecting healthcare organizations while empowering clinicians and other medical staff to do what they want: Take care of patients. Sophos SafeGuard encryption combines the strongest, fastest encryption technology with our deep understanding of healthcare to deliver HIPAA-quality encryption security that does not impact providers' care.

Sophos accomplishes this by listening to our healthcare partners and learning, for example, about increasing the usage of mobile for internal communications within healthcare providers. As a result, we are the only encryption provider that integrates our data protection product with our enterprise mobility management product to give you the ability for secure viewing and editing of sensitive data on mobile devices.

Sophos SafeGuard encryption also delivers:

- **Encryption without performance impact:** Healthcare workers can resist security measures such as encryption if they perceive it might slow down their machine. High-performance encryption technology without noticeable impact on performance makes the process transparent to end users and thus gains users' support. Sophos SafeGuard Enterprise incorporates the latest processors and security technologies so healthcare providers can have data security and speed. In the independent Tolly Test Report, Sophos SafeGuard Enterprise was found to perform faster than competing products from CheckPoint Software, Symantec, and McAfee.

- **Peace of mind in the cloud:** If your healthcare organization uses cloud-based backup or file-share services, Sophos SafeGuard Enterprise helps ensure an additional protective measure by encrypting files before they are uploaded to the cloud-based backup and file-share services.
- **Compliance reporting:** It is not enough to protect patient data; you must be able to produce proof. You need an easy process to demonstrate compliance — and Sophos SafeGuard Enterprise provides compliance reporting that simplifies the process of demonstrating compliance with data security regulations.

Sophos SafeGuard Encryption ensures productivity without disrupting workflow by securing sensitive data wherever it is stored — including laptops, USB drives, network shares, or cloud-based file-share services — with minimal impact on performance. Users typically do not notice any degradation of speed or service, while your organization meets or exceeds encryption and security requirements.

A Look Inside: Sophos SafeGuard Enterprise Modules and Functions

The best security solutions are deceptively simple: Clinicians and other healthcare professionals find them easy to use; years of design excellence ensures dashboards and management tools empower internal or solutionprovider partners to effortlessly implement and manage SafeGuard Enterprise. Yet packed behind the attractive user interface and seamlessly integrated encryption tools are powerhouse security capabilities such as:

Full disk encryption: Protects data stored on desktops and laptops via transparent encryption of the whole drive, including the operating system. This protects users and the healthcare organization from data leakage in the case of lost or stolen laptops.

Centralized management console: Available for all platforms — including Windows-based and Macintosh computers, and self-encrypting disks (Opal1 /2) as well as mobile operating systems iOS and Android — Sophos' centralized management console improves productivity and security by giving security or IT teams one holistic way to see the encryption story.

Removable media encryption: Protects data on removable devices, such as USB sticks and optical media, which is especially critical in healthcare when many patients share results or data from other physicians via potentially vulnerable removable media.

Encryption for cloud: Secures data that's stored in cloud-based backup services (such as Egnyte or Carbonite) and file-sharing (such as Dropbox or Box).

Secure internally shared files: Individuals can securely share folders and files, even large image files, among colleagues and across networks.

User management: Sophos' solution makes sure only the right people have access to encrypted resources such as files, folders, and emails, dramatically reducing the risk of unauthorized access to sensitive information and creating an audit trail in the case of a review.

"For healthcare, I believe there is a definite need for encryption in general. For our organization, we know that Sophos and SafeGuard Enterprise allow us to go beyond the basics so we can encrypt based on our needs, such as full-disk or removable media, without ever compromising the work we do with our patients and the community," said Jeff Barding, senior security administrator at Pomona Valley Health Centers.

Conclusion

Encryption goes a long way toward helping healthcare providers meet HIPAA requirements, especially HIPAA's Security and Privacy mandates. While encryption is not yet mandated, some pundits predict it will be and those healthcare organizations that already have encryption in place will be ahead of competitors. They certainly are in the eyes of patients and employees, who often view investment in encryption and other security measures as a reflection of a caring, engaged healthcare organization.

Not all encryption solutions are the same. Providers should choose an encryption solution that combines speed and security capabilities from a well-established, well-rated industry leader that understands both security and healthcare. Sophos SafeGuard Encryption Enterprise makes healthcare security simple and powerful, delivering the cure for providers' PHI protection ills.

Additional Tips for Data Security

1) **Prevent unauthorized use of USB thumb drives**

   Sophos Endpoint Protection Advanced includes device control capability. Consider creating a device control policy that prevents the use of unauthorized USB drives. Or further tighten security by combining that policy with SafeGuard's removable media protection, which automatically encrypts removable media.

2) **Protect data on mobile devices**

   Today, many healthcare professionals view and respond to patient email via smartphones or tablets. It's wise, then, to consider deploying Sophos Mobile Control Advanced to secure data residing on mobile devices.

   - Fully or selectively wipe the device in case of loss and theft.
   - Set a passcode and other security settings on the device.
   - Configure VPN to securely communicate with companies' servers.
   - Secure Workspace allows the seamless viewing of material encrypted with SafeGuard Enterprise.

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing complete security solutions that are simple to deploy, manage, and use that deliver the industry's lowest total cost of ownership. Sophos offers award winning encryption, endpoint security, web, email, mobile, server and network security backed by SophosLabs—a global network of threat intelligence centers. Read more at www.sophos.com/products.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

2015-12-07 WP-NA (MP)