

IT Health Check

Protecting Patient Data in Compliance with Regulations

Unlike large medical centers, the first things I notice when I walk into my neighborhood physician's office are the many pictures of patients on the wall and the familiar faces of the office staff who know you by name. The clinic's personalized approach is also focused on one thing—the well-being and care of its patients.

But the business of improving the quality of care and saving lives is not so simple. Healthcare is one of the most complex and highly regulated industries, mainly because of the Health Insurance Portability and Accountability Act (HIPAA). In addition, the Health Information Technology for Economic and Clinical Health (HITECH) act was introduced in 2010 to provide financial support for the adoption of electronic medical record systems. Electronic records enable healthcare providers to quickly access patient data, but it also places increased responsibility on these providers to protect patient records from security breaches. In its recent **“Benchmark Study on Patient Privacy and Data Security,”** Ponemon Research found that data breaches cost healthcare providers \$6 billion annually.¹

By Courtenay Troxel





With healthcare reform a top priority, small and midsize business (SMB) healthcare providers are faced with going from having just enough computers for the finance department to everyone having access to systems and data. This article details how

It's all about the data

Providing quality care for patients comes down to data—collecting it, sharing it, and accessing it. From a technology standpoint, it means having the ability to store, protect, and manage the availability of patient information securely,

“Symantec Endpoint Protection is the primary software we depend on to keep our clients up and running...”

– *Jeb Gardner, Support Specialist, The SoundSide Group*

SMB healthcare providers are tackling the changing IT landscape and complying with regulations.

Marc Holland, vice president of market research, HIMSS Analytics, explains: “This dynamic regulatory environment can be very challenging for many SMB healthcare providers. But the changes in healthcare regulations also represent opportunities to get funding for IT projects and, most importantly, to improve patient care.”

along the continuum of care. As a result, SMB healthcare providers face increased security risks when it comes to electronic protected health information (PHI) for their patients such as understanding where the data is, maintaining and transmitting the data, and who has access to it.

To address IT security means a fundamental shift in culture, which starts with people and processes. According to Symantec’s **Internet Security**

Threat Report, Volume XV, healthcare ranked as number two targeted industry for attacks, with 60 percent of data breaches unintentional.²

“Electronic files, if properly managed, can be inherently more secure than paper records,” notes Holland. “Security should be a top priority not only for IT but for all employees.” According to Holland, the following are key factors that an SMB healthcare organization needs to consider to enable an effective security policy:

- > User training, including awareness of relevant state and federal legislative provisions and associated civil and criminal penalties and ongoing refresher training
- > Effective password management
- > Role-based security
- > Encryption of data
- > Annual penetration testing

Educating the staff

Washington County Hospital (WCH), a critical access hospital in North Carolina,

 **Webcast**
The True Cost of a Healthcare Data Breach.



Steven Porter, Chief Information Officer, Touchstone Behavioral Health

“I consider Symantec a trusted vendor because they understand that our needs in the SMB health-care space are the same as larger enterprises.”

– Steven Porter, Chief Information Officer, Touchstone Behavioral Health

WCH materials management director and IT director Christina Craft is in charge of purchasing and maintaining everything from band-aids to equipment needed for the facility. Craft is also a one-person IT shop. Although WCH still has a paper trail, its accounts receivable, payroll, radiology images, and some patient data are now being processed electronically.

“Our biggest challenge is getting all our medical records online, a process that is incredibly complicated,” says Craft. “I have to find the funding, time, and energy to make everything digital, train our staff, and meet HIPAA requirements, all while making sure our patients healthcare needs come first.”

Craft’s top priority is to deliver high quality patient care through improved

staff productivity and efficiency. “Moving patient records from a paper and physical filing system to computers will enable our providers to quickly access and share up-to-date patient information to facilitate more accurate diagnoses, which in an emergency can be life-saving,” Craft notes. “While the benefits of electronic health records promote improved quality of care, I also need to consider the importance of protecting patient data.”

Recently reported in *Health Data Management*, a clinical facility in Indianapolis learned that its employees unintentionally revealed their email login information to third parties, according to the notice. As a result, the third party was able to access certain email accounts within the facility that contained protected health informa-

prides itself on offering the latest in technological advancements in health-care. The 49-bed, critical care facility has been providing healthcare services to Washington County and its surrounding communities for over 60 years.





Kurt Smith, Systems Security Officer, HealthDataInsights

“PGP... helped to define encryption standards that are ahead of even government requirements.”

– Kurt Smith, Systems Security Officer, HealthDataInsights

a different way and must be trained on processes such as how to deal with spam email that may contain malicious viruses or phishing attacks. “We have different levels of security,” Craft explains. “Our staff has access to information depending on their job title and what their function is when it comes to patient data.”

Security and data protection keeps things operating smoothly

To secure and protect its network of 98 workstations and 158 users running Microsoft Exchange Server, WCH relies on Symantec Partner The SoundSide Group and security and data protection solutions from Symantec.

With Symantec Endpoint Protection, The SoundSide Group is able to monitor the network, view each indi-

vidual machine for potential threats, and prevent attacks to keep WCH operating effectively. “People often surf the Internet and click on things they shouldn’t, which can contribute to data breaches,” notes Jeb Gardner, support specialist, The SoundSide Group. “Symantec Endpoint Protection is the primary software we depend on to keep our clients up and running, and we’ve never had an outage with any system running Symantec Endpoint Protection.”

To safeguard systems in the event of data center failure, The SoundSide Group also uses Symantec Backup Exec System Recovery to protect WCH’s critical data and to restore mailboxes and emails on their Microsoft Exchange



Webcast

HIPAA/ HITECH
Security and Privacy
Made Simple.



Server. “We use Backup Exec System Recovery as a business continuity tool, which helps me sleep at night,” Gardner states. “While Backup Exec System Recovery restores files quickly, we have never had to use this feature.”

Going paperless securely

The move to electronic medical records (EMR) gives SMB healthcare providers access to critical patient data at a moment’s notice; keeping that information secure is the challenge.

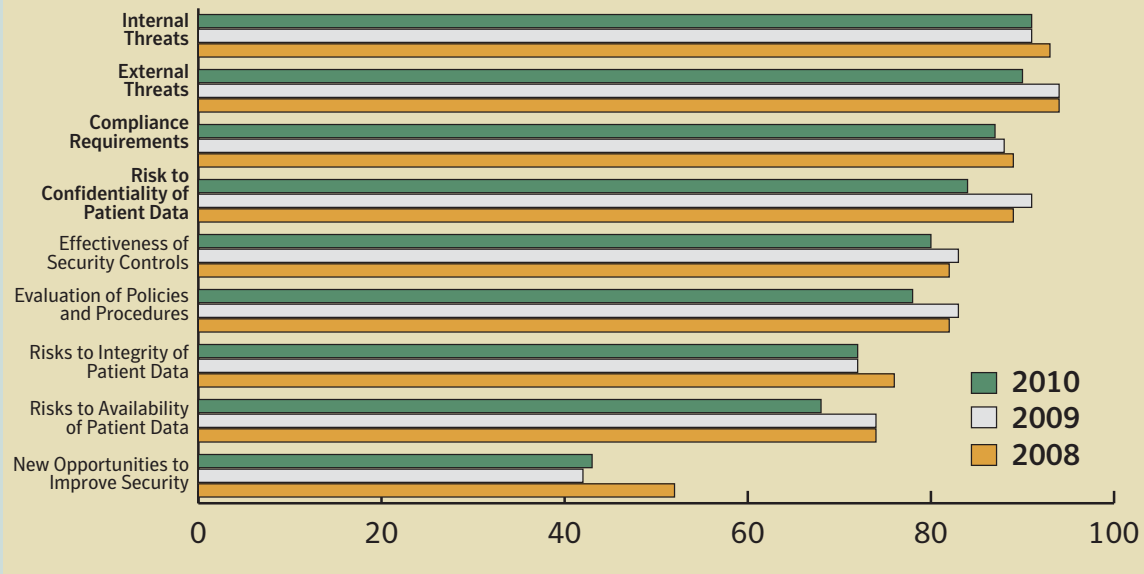
For Phoenix, Arizona-based Touchstone Behavioral Health, an EMR system gave them the ability to deliver improved patient care and better support to the therapists and counselors who provide outpatient, home treatment, and pre-

Start With a Risk Analysis

“The increased focus on protecting patient data and new industry regulations mandating frequent certifications and time-consuming audits, along with limited resources to develop and implement a security strategy, SMB healthcare providers are faced with IT environments that are becoming more complex,” says Marc Holland, vice president of Market Research, HIMSS Analytics.

According to Holland, healthcare providers should start with a risk analysis, also required by HITECH. Every organization is going to be different, including the risks. A risk assessment allows healthcare providers to understand their environment—what they’ve got today and how they want to use data going forward—then look at where the risks and vulnerabilities are, prioritize the issues identified, and fill in the gaps to make sure it’s protected and secure.

Components of a Formal Risk Analysis



Source: 2010 HIMSS Security Survey, November 3, 2010



“The changes in healthcare regulations also represent opportunities **to get funding for IT projects and...improve patient care.**”

– Marc Holland, Vice President of Market Research at HIMSS Analytics

ventative services to children and their families. The EMR system also enables real-time access to the latest updates on patient records, allowing therapists to provide a more personalized and meaningful session for their clients—from anywhere.

To ensure the security of its data, network, and staff in the field, Touchstone Behavioral Health leveraged Symantec Endpoint Protection. “With end users, my biggest security threat, the EMR process involved training our mobile staff on computers and reminding them that security is really their job,” says Steven Porter, chief information officer, Touchstone Behavioral Health. “The nature of the work and the dedication of the staff mean they’re out at the fringes of the Internet looking for solutions to solve very serious and

specific behavior issues, and the research sometimes leads them in areas you may not normally think of going.”

Time saved avoids fines, improves billing cycle

Touchstone Behavioral Health relies on Symantec solutions to help reduce the audit report times, avoid potential fines, and meet the security audit requirements set by HIPAA.

Symantec’s Endpoint Protection console provides a snapshot of Touchstone Behavioral Health’s endpoint security status—a dashboard of when machines last checked in, their A/V signature dates, potential risks, and current threats. The weekly update allows Touchstone Behavioral Health to drill down to specific events or hardware to analyze the root cause and remediation, without digging

through multiple log files or screens, and is sufficient for most audits.

“The reality is HIPAA security compliance isn’t about the actual machines, it’s the report you give to the auditor,” Porter explains. “We’ve been able to reduce audit preparation time to a few minutes and more importantly, reduce the HIPAA report creation from 10 hours down to 30 minutes with Symantec Endpoint Protection.”

With Symantec security solutions enabling the EMR platform, Touchstone Behavioral Health has also reduced its billing time 17-fold through the electronic collection of updated medical records and signatures required upon completion of the visit. “We’ve gone from a billing cycle of 53 days down to three,” Porter notes.

Safeguarding data beyond endpoints saves money

Keeping protected health records secure as mandated by HIPAA goes beyond endpoints. Touchstone Behavioral Health safeguards its data with Symantec Backup Exec in the event of



disaster or data center failure, citing a 97 percent success rate for backups and a 100 percent success rate for restores. “Symantec Backup Exec is a key component to my disaster recovery and business continuity plan.” Porter says.

As the IT environment evolved to virtualized servers and disk-based backups, Touchstone Behavioral Health upgraded its backup strategy with Symantec Backup Exec 2010. The integrated deduplication capabilities in Backup Exec 2010 significantly reduced redundant data that can occur with virtualized environments.

“Deduplicating our data with Backup Exec 2010 has increased our backup speed dramatically,” Porter says. “We’ve gone from a 14-hour backup window to under 3 hours—allowing us to avoid network latency issues during production hours.”

In addition, its ability to provide single-instance storage of its virtualized server data enables Touchstone Behavioral Health to save time, lower storage costs, and minimize backups.

“I consider Symantec a trusted vendor because they understand that our needs in the SMB healthcare space are the same as larger enterprises,” Porter concludes. “And they continue to provide us with the same enterprise-class solutions, which ultimately helps us deliver higher quality care to our patients.”

Encryption: the missing link

One of the requirements of HITECH is data breach notification, which means if a healthcare provider improperly discloses protected health information, the healthcare provider must notify the affected patients within 60 days of discovering the breach. In addition, if the breach is large enough—over 500 patients—the healthcare provider must also notify the [U.S. Department of Health and Human Services \(DHHS\)](#) and the local media. For breaches involving 500 or more individuals, the DHHS is also obligated to post a notice on a publicly accessible website.



Podcast
SMB Strategies for a Healthy IT.

According to the DHHS, two-thirds of all data breaches reported since this rule went into effect in August 2009 have resulted from the loss or theft of computers or backup media containing protected health information.³

This is where encryption is key. Encryption technology uses a cipher to make information unreadable to anyone except those possessing a key, ensuring that lost or stolen protected health information is not misused. What’s more, under HITECH, the data breach notification provisions are not required if the lost data is encrypted.

According to Holland, the frequency of data loss, the cost of corrective action, stricter regulations, and increased worker mobility are just a few reasons why encryption should be mandatory, not to mention the long-term effects of lost business and tarnished reputation. “Healthcare providers should make sure the data is encrypted not only where it originated, but in each instance where it is transmitted to other authorized users



of the data,” he says. “If encrypted data is obtained by an unauthorized party, it can’t be read or used.”

Encryption drives data integrity

For HealthDataInsights (HDI), a Las Vegas-based business that verifies the integrity of healthcare claims, encryption is required by its high-profile customers—the Centers for Medicare and Medicaid Services, insurance companies, and government agencies such as the U.S. Department of Defense.

To ensure HDI has rock-solid data protection, HDI uses PGP encryption technology from Symantec. “Since we handle medical claims, everything we do has to protect patient data,” says Kurt Smith, systems security officer, HDI. “We have 300 employees working remotely, and if someone’s laptop gets stolen or lost, the damage to HDI would only be the cost of the computer, because the data can’t be accessed.”

For its encryption requirements, HDI uses PGP Whole Disk Encryption, PGP NetShare, and PGP Universal Server run-

ning in Guarded Key Mode for backups, data streams, and files.

“PGP NetShare is one of the coolest features, especially when it comes to corporate documents and contracts,” Smith explains. “With PGP in place, administrators are able to restore files or whatever is required, but do not have access to the data unless the administrator is part of the security group that allows them to view it.”

The keys to unlocking the code

Smith explains the function of encryption keys using the example of the 1983 movie *WarGames*, where one officer has the unlocking code to “turn the key” upon order, and another officer has the key code to validate the order to engage in thermonuclear war. Very simply, encryption requires two keys: a primary key to encrypt information and verify signatures and a private key used to sign and decrypt information. “PGP not only created an encryption product that is second to none, but also helped to define

encryption standards that are ahead of even government requirements,” Smith notes.

A major benefit of PGP encryption technology is the ability to segregate protected health information

COMPANY PROFILES

Washington County Hospital

Founded: 1950
Location: Plymouth, North Carolina
Employees: 152
Website: www.wchonline.com
Symantec Partner: *The SoundSide Group*
www.soundsidegroup.com

Touchstone Behavioral Health

Founded: 1968
Location: Phoenix, Arizona
Employees: 200+
Website: www.touchstonebh.org

HealthDataInsights

Founded: 1993
Location: Las Vegas, Nevada
Employees: 300
Website: www.healthdatainsights.com



on a client-by-client basis. Data is segregated and encrypted under different groups, and privileges controlled based on client data. “PGP paid for itself within the first month of deployment, and it’s a great sales tool, because we can put our customers at ease,” Smith says. Holland notes, “Only encryption protects the data itself no matter where it is used, stored, or transferred.”

With the new regulations and enhanced data policies, healthcare providers are able to improve staff productivity and efficiency, and are able to access and share updated real-time patient medical records from anywhere. Ultimately, it’s the patients that benefit from the overall improved quality of care. ■


¹ *Benchmark Study on Patient Privacy and Data Security*, Ponemon Institute, November 9, 2010.

² *Symantec Global Internet Security Threat Report*, volume XV

³ *U.S. Department of Human Health Services*

⁴ *2010 HIMSS Security Survey*, November 3, 2010

Courtenay Troxel is managing editor for The Confident SMB and CIO Digest and manager of online content and newsletters at Symantec.



What if a laptop is lost?

PUT SECURITY FIRST.

Learn about Endpoint Encryption ▶

