Enabling Secure Collaboration in Healthcare

Compliance directives brought on by the HIPAA Omnibus Rule and HITECH Act are bringing increased scrutiny to healthcare organizations. The need for infrastructure and tools that enable secure collaboration for everyone that handles protected health information (PHI) has never been greater. However, most healthcare organizations are challenged to provide the IT expertise and resources to deploy and manage complex infrastructures and cloud / mobile integrations on their own. Employees are reaching for consumer-based tools to get their jobs done, and that puts healthcare-affiliated businesses and agencies at risk. What’s the best way to ensure compliance, enable collaboration and boost productivity in healthcare? This paper examines current challenges in the healthcare compliance landscape and provides the answers healthcare professionals need to ensure control, compliance and visibility across their organizations.

Unfortunately, too many healthcare organizations feel like their data is secure enough — or that the costs and complexity of instituting appropriate security solutions or undergoing an in-depth risk assessment aren’t worth the effort, but the consequences of non-compliance can be devastating.
The Shifting Healthcare Compliance Landscape

The six-month grace period for HIPAA Omnibus Rule compliance came to an end on September 23, 2013, and new changes brought on by the HITECH Act are impacting the healthcare privacy and security landscape. Today, it’s not only traditional healthcare providers, such as public and private healthcare organizations, hospitals and physicians’ offices that must comply with healthcare security directives. Nearly every business that handles protected health information (PHI) on behalf of HIPAA-covered entities, including business associates, consultants, service providers and their subcontractors, must now comply with established privacy and security controls for notification, consent and authorization. Failing to do so can translate to both civil and criminal penalties, costly fines and damaged reputations.

“Unfortunately, too many healthcare organizations feel like their data is secure enough — or that the costs and complexity of instituting appropriate security solutions or undergoing an in-depth risk assessment aren’t worth the effort, but the consequences of non-compliance can be devastating,” notes Atif Chaughtai, Director of Security for Axway.

Healthcare organizations simply can’t afford to ignore how patient data and confidential information is protected, shared and disposed. This is clearly evidenced by the U.S. Health and Human Services (HHS) Data Breach Wall of Shame, which shines a negative spotlight on organizations that fail to properly encrypt and protect patient data. There you’ll see hundreds of examples of the escalating costs of violations, totaling $10 million in 2012 alone. This year the Wall of Shame included a data breach by a large organization that resulted in fines totaling over $1.2 million for exposing the protected health information of over 350,000 individuals.

“The vast majority of large-scale data breaches in the last five years are associated with carelessness rather than malevolence, said Chaughtai. “We’ve all heard stories of stolen back-up tapes, employees losing a USB drive that contained patient data or not understanding exactly how to run a portal and leaving confidential files open on a server.” There are a number of unavoidable business factors making it more difficult for even the most well intentioned healthcare organization to avoid potential missteps. As organizations work to ensure the safe exchange of private healthcare, administrative and financial information, they’re challenged by business factors such as an increasingly mobile workforce, the expanding number of healthcare business associates subject to regulations, a reliance on email for collaboration and the understandable desire to operate as fast as possible.
As in every industry, there is a need within healthcare to collaborate quickly and efficiently. The difference with healthcare is that the data that needs to be shared among and between participants, be they providers, payers or patients, is very sensitive and highly regulated by the rules for sharing Private Health Information (PHI). “While it’s easy to see increasing government regulations and the push to transition to electronic health records (EHR) as inconvenient, they are intended to protect patients and improve health outcomes while lowering the long-term costs and complexity of healthcare in the U.S.,” said Chaughtai. “Health IT has arisen to facilitate these goals and encompasses a whole set of systems, tools, processes and policies that work together to let people collaborate in a safe and secure way.”

**Addressing the Human Element**

Healthcare is ahead of the curve in terms of using technology for automated transactions such as billing and insurance claims. “Most large-scale healthcare organizations, labs and insurance providers use specialized tools, such as electronic medical record solutions and standardized practices, to protect patients’ data as it flows from agency to agency,” said Dave Butcher, Director Solution Architecture, Security Solutions Group, Axway. “However, there are no standards for exchanging data with patients, and the language in the HIPAA Omnibus and HITECH rules regarding Business Associates introduces questions and potential complications for electronically sharing healthcare-related data.”

The majority of healthcare consumers simply don’t have immediate access to a secure EMR or EHR system, but they may want a copy of their lab results delivered to them while they are traveling or need a copy of their MRI data to get a second opinion. Most challenges arise from ad hoc interactions and required collaboration due to the human element in healthcare, one that obviously can’t be eliminated but can be addressed. The question for Health IT becomes: How do we get data from point A to point B electronically, safely and easily.

“There is significant value in recognizing that everyone uses email today, and ad hoc communications will occur at every level of an organization,” said Chaughtai. “Health IT departments must find the balance between mitigating risk while enabling productivity, and the intersection of compliance and collaboration is difficult to navigate. End-users certainly can’t be left to their own devices when it comes to exchanging healthcare data. If systems and tools are too difficult or impede fast interactions, no one will use them, and ease-of-use is often the reason people reach for consumer-based file sharing tools that are not ideally suited for healthcare.”
While an organization may intend to protect the safety and privacy of health records, without a system that enforces their set policies, it’s very easy for even the most well-intentioned individuals to forget the rules or take shortcuts that they shouldn’t.

**HIPAA-Compliance: It’s a Process, Not a Product — And Policy is Essential**

While some consumer-based tools, such as Box, claim to be HIPAA and HITECH compliant, the fact is that there is no one piece of software, cloud-based or otherwise, that on its own can ensure regulatory compliance in healthcare.

“HIPAA does not certify individual products, and the label HIPAA-certified is a misnomer,” notes Butcher. “HIPAA regulations are a broader set of definitions, training, guidance and policies that provide a framework designed to help organizations ensure compliance.” An organization can’t simply install a security solution, set up a data center or roll-out software, then claim HIPAA-compliance. There are recommendations in place for healthcare-affiliated organizations to follow, and all of the regulatory agencies recommend starting the journey toward HIPAA compliance with a risk assessment, and then develop policies to secure and protect health records and healthcare-related data from both inadvertent and malicious disclosure.

“In the world of healthcare, policies are essentially intentions,” notes Chaughtai. “When you consider the number of temporary hospital workers or service-related subcontractors needing access to healthcare data, it’s easy to see why it’s important for organizations to have a way to ensure that their intentions are followed consistently. While an organization may intend to protect the safety and privacy of health records, without a system that enforces their set policies, it’s very easy for even the most well-intentioned individuals to forget the rules or take shortcuts that they shouldn’t.”

Consumer-based tools, such as Box, often lack the ability to define and enforce such policies — and while they may provide SSL encryption for data in motion, they also hold the keys used to encrypt the data. This means that the cloud provider can decrypt your data, and encryption keys can be shared across tenants in the cloud. Encryption is essential for secure collaboration in healthcare. Should an organization have a data breach or accidental disclosure of non-encrypted data, it is obligated to report it and may be subject to fines and penalties up to $1.5 million. If the government decides that the organization lacked appropriate policies and protections, including encryption, class-action suits can be filed with any state’s Attorney General, reaping additional money that can be shared with any whistleblower.
On the other hand, if data is lost, mishandled or stolen in transit, but was encrypted according to the FIPS 140-2 standards, it's as if the data breach never occurred. This is because of the belief that the data can't be unencrypted quickly enough or easily enough to make it possible or feasible for it to be misused. If encryption is going to meaningful, organizations must also be able to manage identities and only share keys among trusted partners. Keeping encryption keys private and unique across users of the system ensures that no potential for key reuse exists, eliminating the threat of cross-tenant data exposure.

**Reaching for the Cloud**

While cloud computing holds great promise for cost savings and collaboration, many healthcare organizations have been reluctant to go to the cloud. “While there are available security measures and encryption for cloud that make it an extremely viable option for secure file sharing and health IT, many agencies have been reticent to leverage cloud computing because, in a public or even hybrid cloud, data is often co-mingled,” said Butcher. “A private cloud with data segregation is a better option for healthcare.”

Setting up a compliant data center or designing and deploying a private cloud is a complex undertaking and one that many healthcare organizations don’t have the time or experience to undertake. “Small organizations simply don’t have the manpower and larger companies often don’t want to dedicate the infrastructure they already have to cloud computing, given that the infrastructure for a majority of hospitals is already 95% purposed,” said David Shepard, EVP of Sales and Marketing for BroadCloud, a leading managed IT infrastructure provider that offers colocation, dedicated servers and managed infrastructure to businesses around the world.

“Ask a healthcare organization about their areas of expertise and they will most likely point to patient care or a specific surgical area or specialty, such as oncology or cardiac care — not IT,” said Shepard. “By relying on IT experts to deliver geographically diverse, secure and compliant hosted private cloud, healthcare organizations of all sizes can focus on what they do best while reaping the benefits of a hassle-free cloud infrastructure that can enable secure collaboration and instant regulatory compliance.” With the flip of a switch, there is more storage and computing capacity available. By running secure collaboration solutions such as Axway’s DropZone™ and MailGate SC™ on top of that infrastructure, securely sharing a three-dimensional graphics-heavy diagnostic oncology image is not a concern, and HIPAA and HITECH compliance is ensured.
“BroadCloud and Axway are working together to lessen the pressure on healthcare providers to secure data at rest and in-transit, and to ensure compliance,” said Bryan Turbow, CTO and founder of BroadCloud. This partnership can help healthcare organizations save time and money and reduce risk by allowing them to rely on established healthcare IT experts instead of trying to become cloud computing or security experts themselves. Plus, both BroadCloud private hosted clouds and Axway’s DropZone and MailGate SC integrate seamlessly with existing architecture and enterprise systems, with no browser or operating system dependencies. This gives healthcare organizations the flexibility to add new levels of security as their needs change, without making changes to established systems, applications, protocols or end-user workflows.

Unlike hosted solutions that add complexity or fail to integrate with existing infrastructure, BroadCloud and Axway design solutions with security, simplicity and integration in mind from the start. “We don’t make organizations go through the process of being re-certified; we can plug right into a healthcare agency’s existing infrastructure, leverage existing security tools, log-in systems, passwords and secure access authentication methods,” said Turbow. “Our easy-to-use solutions work with and expand the capabilities of our clients’ existing computing, compliance and security architectures, all of which translates to substantial savings.”

BroadCloud also streamlines healthcare compliance audits by providing active monitoring and visibility to see exactly who has accessed data, and when they have done so, it’s easy to provide an assessor with an audit trail.

A Direct Path to Secure Collaboration

As the first truly secure enterprise collaboration gateway and platform, Axway DropZone and MailGate SC provide healthcare organizations with a secure method to share files, email messages and safely interact with internal and external collaborators from their device of choice. Axway’s Secure Collaboration solution for healthcare requires no additional IT resources for deployment and enables:

- Secure file sharing and collaboration capabilities from anywhere, including desktop, tablet or smartphone – all with enterprise-class policy controls and encryption.
- Policy-based content management and encryption for complete control and visibility into whatever is being shared.
- Comprehensive email hygiene and network protection, including virus protection, anti-spam filtering and dark traffic defenses.
The solution provides multiple tiers of security. The content and network levels can be used individually or in combination to block threats and secure inbound and outbound email traffic, promoting collaboration while ensuring compliance.

“There is simply no other solution on the market that delivers in the three key areas of usability, security and policy control,” said Butcher. “By using a tool such as DropZone with MailGate SC, you don’t have to slow or penalize productivity to reduce your risk. Usage allows healthcare organizations to really take control of ad hoc interactions, ensure encryption, set and enforce policy, and even give users the ability to access information from their mobile devices without undermining the organization’s overall ability to secure data or protect health records.”

To learn more, visit www.axway.com.