MegaPath
A Fusion Company

WHITEPAPER

SECURING SOCIAL MEDIA FOR HEALTHCARE

WITH MANAGED SECURITY SERVICES

THE THREAT: SOCIAL MEDIA DISCLOSURE OF PROTECTED HEALTHCARE INFORMATION

Social media sites—such as Facebook and Twitter—can be a tempting outlet for healthcare employees to discuss patient information that should be private.

Consider these recent incidents reported in the media:

- ER staff who posted photos of patients with unusual injuries.
- A physician who discussed case details in a way that allowed the patient to be identified, even without revealing the patient's name.
- Employees who think it is okay to access and share the health information of friends, relatives, or celebrities.

These breaches of information security and patient privacy may or not be intentional, and they can be committed by an employee, a contractor, a temporary employee, or an external party. However, the repercussions to the organization of a protected healthcare information (PHI) disclosure are significant because these confidentiality breaches violate HIPAA rules about protecting patient privacy and ensuring workforce compliance. Repercussions may include:

- Filing reports with the U.S. Department of Health and Human Services and state health agencies.
- Incurring financial penalties for individuals up to $50,000 and for organizations up to $1.5 million.
- Notifying not only the patient and family members affected, but also the local media, which can negatively impact the organization's reputation and patient confidence.
- Making expensive and time-consuming efforts to remediate the breach, identify the parties involved (and take disciplinary action if appropriate), and retrain staff on organizational policies and practices for social media.

It is important to note that smaller clinics, group practices, nursing homes, and labs are just as vulnerable to unauthorized information releases via social media as are large hospitals.

Motivations behind unauthorized patient data include:

- Curiosity about patient conditions and care.
- Medical identity theft to obtain care or for filing fraudulent insurance claims.
- Financial identity theft to obtain credit card number and account data.

A survey conducted by Ponemon Institute and sponsored by MegaPath found that "… smaller healthcare organizations face the same challenges as larger organizations. Almost every organization has had a data breach and 29 percent believe with certainty that it was likely that the breaches resulted in medical identity theft."

PREVENTING INAPPROPRIATE DISCLOSURE

How can a healthcare organization prevent PHI disclosure via social media? It takes a combination of policies, security technologies, and ongoing monitoring of network and data activity.

Policies Covering Social Media Use

Defining clear and strong internal policies about social media use and disclosure should be your first line of defense in safeguarding PHI from a social media breach. However, in the Ponemon survey, 55 percent of the respondents don't have an acceptable use policy for activity on social networks. You'll find examples of social media policies established by healthcare organizations at: http://ebennett.org/?s=social+media+policy.

HIPAA Requirements for Technical Safeguards

After policies, the next focus should be on implementing network security technology. To comply with the HIPAA Security Rule, a healthcare organization must implement several technical safeguards for controlling electronic access to and transmission of PHI:

- Controls that limit electronic PHI (e-PHI) access to only authorized persons.

- Logging capabilities that allow audit of access and other activity in electronic systems that contain or transmit PHI.
- Protections to ensure that e-PHI is not improperly altered or destroyed.
- Measures that guard against electronic snooping or access to e-PHI as it is transmitted over a network, whether an enterprise network or the Internet.

The "Safety Net" of Network Security Technology

A technology "safety net" can help to meet the HIPAA Security Rule requirements, prevent breaches when employees don't follow policies, and provide tools for monitoring network activity. Achieving this safety net involves implementing multiple technologies and practices for securing data, applications, and the enterprise network, including Internet access.

URL Filtering (White/Black Listing). The most basic network security technique is to block access to social media sites entirely via URL filtering. However, this complete restriction isn't always appropriate and in many cases it can be bypassed by a determined user. Yet URL filtering is an important tool to have in place when circumstances warrant.

Web application control. A more effective way to control social media access and activity on the enterprise network is through Web application control capabilities. This control analyzes port 80 (Internet) traffic, determines its content, and restricts how Web-based applications are used. For example, you can allow use Web application control to users to view Facebook, but restrict their ability to post to their pages or upload photos or video.

Traffic Logging. Traffic logging technology records all data sent over the Internet from your office(s), helping with HITECH Act compliance and giving you essential information for monitoring, auditing, and troubleshooting network activity—including social media. To be effective, this capability should support packet-level logging for web application traffic. And, as part of your policy training, make sure users are aware that all of their social media interactions are logged. This measure can serve as a strong deterrent against posting patient information because employees won't be able to deny doing so.

Data Leak Prevention. In addition to general social media control, you can also block specific patterns of data from leaving your network using Data Leak Prevention (DLP) capabilities in a network security solution. There are obvious types of data—such as patient IDs, beneficiary numbers, social security numbers, and credit card numbers—that should never be transmitted via social media or web-based email applications.

Then there are non-obvious patterns and types of data. HIPAA defines PHI using 18 specific identifiers, which may in combination reveal a patient identity. For instance, a birth date on its own may not identify a patient, but when combined with a zip code and an admittance date, a patient may be easily identifiable. DLP technology can be set up to use compound rules that look for and block two or more data items in a transmission—such as dates that are more than five years in the past (indicating a possible birth date) combined with a phone number, email address, or zip code.

These types of strong information security capabilities require appropriate systems as well as expert security staff, making them expensive to implement and manage in-house. The cost and expertise required can be an especially large hurdle for a clinic, multi-physician practice, or similar small-to-midsize healthcare organization.

Instead, affordable and effective security management for social media and other network activity can be obtained from a Managed Security Services (MSS) provider—such as MegaPath.

PROTECTING NETWORK AND DATA SECURITY WITH MANAGED SERVICES

Whether based in the service provider's cloud or on your premises, a Managed Security Services (MSS) solution provides a comprehensive, multi-layered approach to network security that helps protect your systems and patient data while maintaining security compliance. MSS can also coordinate the alerting, logging, reporting, compliance, and response activity that are vital for maintaining and controlling social media access via your network. These services can be fully implemented in the cloud, at your premises, or in a hybrid configuration.

IN SUMMARY

All MegaPath MSS are designed to assist healthcare delivery organizations in meeting HIPAA standards, including those imposed under HITECH. MegaPath MSS also deliver essential capabilities for meeting the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF).

MegaPath services are delivered in a Software as a Service (SaaS) format, which means there is no hardware to acquire, no OEM software contracts to purchase, and services can be provisioned on demand.

MegaPath is a leading cloud communications company that empowers businesses to easily and securely communicate between their headquarters, employees and business partners. The company offers a comprehensive portfolio of voice, unified communications, Internet connectivity, and hosted IT services. In addition, our secure data networking services provide secure multi-site and remote access connections to empower today's healthcare organizations.

NEXT STEPS

Visit www.megapath.com/security to learn more about MegaPath Managed Network and Security Services solutions. Or call a MegaPath Business Consultant today at 1-877-634-2728.