Protecting and Securing Privacy Data and Sensitive Information in Today’s Healthcare Organization

McAfee® Network Data Loss Prevention

The IT staffs of healthcare organizations struggle daily with the challenge of achieving compliance with the Health Insurance Portability and Accountability Act (HIPAA) and their own internal policies, protecting sensitive data, and ensuring appropriate use of the network.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which took effect in April 2003, has had a huge impact on healthcare organizations. Created to strengthen privacy protection for personal medical information, HIPAA governs the storage, access, and transmission of patient health data. Failure to meet HIPAA regulations can result in fines of up to $250,000 and 10 years in prison for corporate officers. An even greater threat, however, is the damage to the organization’s brand and reputation should a privacy breach become public.

In addition to HIPAA, healthcare organizations have evolved their own internal guidelines and policies for protecting sensitive information and regulating the appropriate use of the network, the web, and email by employees.

How can IT professionals at healthcare organizations ensure compliance with external and internal policies and protect valuable patient health information? This document identifies a number of areas of concern and describes how McAfee Network Data Loss Prevention (DLP) helps IT professionals discover sensitive data at rest, monitor traffic in real time, and capture events for after-the-fact investigation.

The challenges: protecting data

Sensitive information beyond the control of IT
Referring physicians regularly share clinical information with their private practices, resulting in unencrypted patient health information (PHI) that resides on systems beyond the monitoring and control of a healthcare organization’s IT staff. Also beyond the radar of IT may be clinical trials in progress that generate volumes of proprietary information (i.e., intellectual property) that must be protected—yet IT is unaware of its presence. With or without full knowledge, IT staff bears responsibility for maintaining HIPAA compliance and making sure that PHI and sensitive information are protected.

Managing the tsunami of information
The ubiquity of computers and the Internet has made the ability to share digital information commonplace. But this has created a new challenge for IT professionals, especially those in the healthcare industry who must enforce strict regulations on data protection. The massive volume of information flowing across networks has hindered healthcare organizations from effectively locating and cataloging sensitive data and protecting it, whether it resides on file servers or laptops. Knowing who should have access to this data or who it should be sent to is just another component to add on top of this already daunting information security challenge.
Guarding sensitive information assets
Patient health information is clearly defined. Healthcare organizations know what to look for and know they need to protect it. However, what constitutes sensitive information is not as clear, yet it must be just as stringently protected as PHI. How then can organizations protect their sensitive information when they don’t always know what it is? Generally, just when they do begin to understand it and have a protection strategy in place, another new data type emerges. Or after interviewing all business stakeholders and developing a map of which partners should have access to what data, new partners emerge. Knowing what to protect, and from whom requires considerable and continuous manual effort. How do organizations stay current and keep critical assets from getting into the wrong hands?

Enforcing acceptable-use policies
In spite of the best efforts by healthcare organizations to educate staff, some employees will distribute over the network or download materials that they may or may not be aware are inappropriate and prohibited by internal use policies. Compliance with web and email appropriate-use policies is an ongoing issue with nearly all healthcare organizations. Employee downloads of pornography, movies, or MPEG files are common. How does IT make sure that employees follow the company’s acceptable-use policies without choking off access to nearly everything?

Understanding potential risk
Weak enterprise network device configurations can pose major security vulnerabilities for healthcare organizations. Laptops, mobile phones, and PDAs can allow sensitive data to leave the network, while security applications such as firewalls, intrusion prevention systems (IPS), and intrusion detection systems (IDS) may give organizations a false sense of security as not all threats come from outside the organization. How do healthcare IT professionals ensure that their company is not at risk, or determine the extent of the risk if, for example, a laptop is lost or stolen?

Solution: The intelligent approach to data protection
Protecting against a HIPAA breach—the data you know should be protected
McAfee Network DLP identifies PHI, such as medical records, social security and bank account numbers, credit card and driver’s license information, and login and password credentials, wherever it resides. Our predefined rules for HIPAA data help organizations easily determine where any PHI or personal identifiable information (PII) is stored, where it is going, when it has left, and who it is being sent to. We uncover information flows outside of what is normal, such as unusual transfers of data files to the wrong individuals, images of high-profile patients being sent through webmail, or discussions of private patient information over instant messaging. We help organizations set policies and rules establishing who may access the data, who may receive the data, and who may send it out. McAfee Network DLP blocks the data from being sent, or allows data to be sent selectively to individuals. With McAfee Network DLP, organizations can implement policies and uncover the broken practices beyond what they know.

Maimonides Medical Center (MMC) in Brooklyn, New York, employed McAfee Network DLP to uncover problems with how its physicians were sharing PHI with their private practices. The hospital has built an industry-leading example of how to comply with HIPAA policies and procedures. Patient data is protected, and MMC has realized significant cost savings by moving patient records from paper to electronic formats.

Ensuring adherence to acceptable-use policies
McAfee Network DLP identifies inappropriate data as it traverses the network, enabling IT staff to intercede with those responsible. All data flowing in and out of the network is monitored by McAfee Network DLP. Depending upon what type of data it is, McAfee Network DLP determines the destination and whether this information should be leaving the network. If identified as inappropriate, predefined rules can be set to alert the sender’s immediate supervisor, human resources, or legal departments, or
block the transmission. McAfee Network DLP identifies inappropriate materials by actual content, not file names. If employees are sending out pornographic content, the system recognizes it and alerts staff.

MedStar Health, a community-based network of hospitals and healthcare services in the Baltimore-Washington DC region, relies on McAfee Network DLP to detect the use of unauthorized voice over IP (VoIP) internet phone services or the transfer of large video files.

MMC uses McAfee Network DLP’s patent-pending skin-tone image analyzer to find content containing adult images entering the hospital’s network. The risk discovery capability enabled IT to determine where the images went and run a search agent against the IP address to see if it had received other web pages containing adult content. McAfee Network DLP allowed MMC to uncover and virtually eliminate these problems.

Learning how to protect your sensitive information
Organizations can’t protect what they don’t know about, right? Wrong. McAfee Network DLP offers the only solution available that helps IT staff learn where sensitive IP is and what their sensitive information is—they no longer have to guess. Whether sensitive information is on laptops, shared file servers, local machines, or in document management systems, we help determine what is sensitive and how to best protect it, and mitigate risk.

Because McAfee Network DLP captures historical information, IT organizations “learn” through mining of all communications. Staff can uncover information quickly to determine what data is sensitive, such as a new clinical trial. This historical data can be mined to identify flows that are outside of what is considered normal, such as unusual transfers of sensitive information to the wrong people, pictures of high-profile patients being sent through webmail, or discussions of private patient information sent over instant messaging.

Armed with this new information, IT can update or modify rules and policies to cover inappropriate data flows previously unaccounted for in a much more expedient manner. Furthermore, as new rules are created based on what was learned from historical data, organizations can test them in real time against historical data to validate their accuracy prior to going into production.

McAfee Network DLP helps companies to analyze both the content and the context of their sensitive information and communications. All of it—and with a high degree of efficiency, speed, and adaptability.

MedStar leverages McAfee Network DLP’s capture and search capabilities to learn how users are using the network, what kind of information they are sending and receiving, and who information is being sent to. The administrator can easily query the capture database to identify HTTP responses, message attachments, or image files of a specific size or size range, in efforts to understand what activity a user may be engaging in, or if rules need to be adjusted. The capture capability provides key insight into the network to see what activity is in violation of internal acceptable use policies, regulations, or involves transmission of sensitive internal information.

Knowing your risk potential
McAfee Network DLP identifies weak device configurations, so IT staff can correct them and secure the network. McAfee Network DLP Discover fingerprints all sensitive data so it can be located and protected. By identifying where sensitive information resides, IT staff can determine whether employees have access to data that they shouldn’t. Or, if the organization knows what information resides on a laptop and that device is lost or stolen, the organization can more fully understand its risk.

MMC has leveraged McAfee Network DLP to identify weak device configurations. Without the information provided by McAfee Network DLP, these holes would have remained undetected. By correcting these problems before they resulted in information leaks, the IT department avoided costly penalties for noncompliance with HIPAA and provided a higher level of security for the hospital.
“The adoption of EHR systems are critical for continued improvements in quality of care, greater efficiencies and management of medical costs. The information created, accessed and stored in these systems and their ability to integrate with health information networks and data exchanges introduces security issues which have not, to date, been adequately addressed.”

eHVRP Board of Advisors

McAfee Network DLP includes advanced software features with a unique “learning” approach. Based on a captured index of communications, the McAfee Network DLP historical index can be used for:

* **Investigations**—Analyze and assess communications by topic, user, or destination
* **Rule Tuning**—Test new rules against historic archives to ensure accuracy without having to tune them over time
* **Data Mining**—Use analytical techniques to analyze communications to understand what rules are necessary
* **Policy Creation**—Enables associations, clustering, and advanced analysis techniques to understand who is sending your sensitive information out, how it is being sent, and where it is going

**Summary**

With the continuous threat of security breaches that can result in fines, penalties, and long-term damage to a healthcare organization’s brand and reputation, data loss prevention is a solution that all health organizations should have to protect sensitive data and mitigate risk. With McAfee Network DLP, healthcare organizations can:

* Comply with HIPAA and other regulations
* Safeguard confidential company information, patient health and other sensitive information
* Control information sharing with medical groups and clinical trials
* Protect brand equity and company reputation
* Enforce internal acceptable-use policies
* Eliminate weaknesses in security infrastructure

McAfee Network DLP has pre-built rules for patient health information that help organizations protect the right content. And by monitoring data in motion and scanning data at rest, we literally enable “learning” through mining all communications, not just rule hits. McAfee Network DLP protects the obvious sensitive data, and the not-so-obvious sensitive data that could put an organization at risk.

**Only McAfee Network DLP helps you learn**

Taking a comprehensive approach to information protection, McAfee Network DLP safeguards enterprise assets by protecting obvious information such as patient medical records and Social Security Numbers (SSNs), while allowing organizations to learn about not-so-obvious information that demands protection.

Only McAfee Network DLP provides the performance, accuracy, and comprehensive content classification needed to help you protect all your vital information. For more information about McAfee Data Protection solutions, please visit www.mcafee.com, or call us at 888.847.8766, 24 hours a day, seven days a week.