Healthcare organizations today possess and manage a tremendous amount of sensitive information. From Personal Health Information (PHI) and Electronic Health Records (EHR) to patient financial data, healthcare organizations are responsible for securing these critical data assets from accidental loss or intentional data breaches.

Negative publicity from a data breach can have lasting consequences, undermining patient confidence and damaging an organization's reputation. In addition, as the Obama administration continues to push forward in its effort to modernize the nation’s health care system by making all health records digital, government regulations are being produced and refined to require health care organizations to implement comprehensive security systems to protect patients' sensitive data.

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, got healthcare organizations to start thinking about protecting patients’ sensitive data; however, it had weak enforcement and minimal penalties. With the introduction of the American Recovery and Reinvestment Act of 2009 (ARRA), any organization that possess PHI faces much more stringent data security, privacy, and breach notification policies and the consequences for not complying are significant. Personal health information stored with non-HIPAA entities (e.g. business associates) is now protected.

**Common Avenues for Data Exposure**

As you begin to think about protecting your patients' sensitive data you need to identify the common avenues of how the data is exposed. Most data loss is inadvertent and results from human error or lack of understanding of the organizations data handling policies. Sensitive data may be lost via the network or directly from a desktop/laptop when copied to removable media. In addition, sensitive documents can be found on publicly accessible file shares and employee computers which put them at a very high risk of exposure.

**The Network**  
Data loss via the network is a major type of data exposure in healthcare organizations. Common exposure mechanisms include:

- **Webmail** – Tools like Gmail, Yahoo! and MSN are commonly used by physicians and staff to communicate with patients and external partners, unfortunately these communications channels are not encrypted and can result in patient data exposure.

- **Web 2.0** – MySpace, Facebook, Twitter and other Web 2.0 applications are skyrocketing in popularity and have recently been the avenue for many data breaches.

- **Corporate Email** – Many healthcare organizations have implemented some form of email encryption to meet HIPAA requirements, yet email still remains a common path for data loss. A comprehensive email encryption solution must be combined with the detection accuracy of a DLP solution including automated message encryption services.

- **FTP and Other Network File Transfer Mechanisms** – All file transfer-oriented applications are potential avenues for data loss. Similar to Web 2.0 postings, file transfer applications are utilized by data-stealing programs to transfer sensitive data out of the organization without your knowledge.

- **Unsecured Partner Communication** – Automated communication of patient data is widespread in the healthcare industry. HL7 or X12N messages are transmitted between partners, physician practices, diagnostic labs, and payers for claims settlement. All EDI communications should be encrypted, but in many instances
are not. Healthcare organizations need immediate audit visibility into these unsecured communications, and the ability to block or encrypt the sensitive data being transmitted.

Many of the data leaks Code Green Networks has seen, through its Healthcare Data Loss Assessment Service, have been through the network. Some examples include:

- Entire unencrypted patient databases repeatedly sent out from a healthcare organization to its Hospital Information System (HIS) vendor, as part of system testing.
- Unencrypted patient records sent via webmail
- Nursing staff using Google Docs for patient treatment and status notes, and at the end of their shift transcribing the notes to the internal systems.

The Endpoint
The second channel of data loss occurs when data is moved off endpoint workstations typically to USB drives or other removable media. USB and other removable storage devices are ubiquitous, can hold large quantities of data, and are often difficult to control.

A healthcare system, which Code Green Networks is now assisting with patient data protection, reached out for help after a doctor lost a USB memory stick that contained data extracted from the medical records of hundreds of patients. The CIO from the organization said it was common practice for doctors to put information on memory sticks to be used while working from remote offices.

The Unknown
A healthcare organization’s risk of data loss is directly correlated to the level of control it has over sensitive data. In many organizations, multiple copies of sensitive documents can be found on servers throughout the organization. In many cases these documents can be found on publicly accessible file shares and employee computers which put them at a very high risk of exposure.

As an example of how widespread the problem can be, a Code Green TrueDLP healthcare customer ran an initial patient information discovery scan of several machines on their network. Over 22 million patient records were discovered, located in many easily accessible places including folders on employees’ PCs and laptops, on network servers in folders widely shared throughout the organization, and on open SharePoint servers.

The Discovery function of a DLP solution allows IT to locate sensitive data throughout the organization and regain control over it. As sensitive data is located, it can be moved to a secure location on the network, reducing or eliminating the risk of accidental exposure.

Strategy for Protecting Patient Health Information
Once you understand the common avenues for data exposure, you should begin the process for protecting your organization’s PHI. There are four steps to begin the process for protecting patient data:

1. Identify Structured Data – The first step in protecting patient data is identifying which internal systems hold patient information. The key questions are which systems hold patient demographic information? And which systems identify patient clinical information? Don’t forget extract spreadsheets that might contain this data.
About Code Green Networks

Code Green Networks delivers data loss prevention solutions that protect private employee and customer information and safeguard intellectual property across all electronic communications channels. The company’s easy-to-deploy, easy-to-manage content inspection appliances rapidly detect and prevent potential data leaks, helping organizations automate compliance and mitigate risks from internal breaches that can result in loss of revenue, financial penalties and irreparable damage to a corporation’s image, brand and customer loyalty.

Protecting Your Most Sensitive Digital Assets

Code Green Networks TrueDLP provides organizations with easy-to-deploy and easy-to-manage solutions for protecting confidential data across all electronic communication channels enabling organizations to:

- Ensure compliance with regulations such as ARRA 2009, HIPAA, PCI, and state/federal privacy regulations
- Automatically encrypt emails utilizing policy-driven healthcare data classification and filtering
- Provide unobtrusive enforcement of data loss prevention policies across all popular Internet communication channels
- Utilize HIPAA code sets (e.g. HCPCS, ICD-9, LOINC, and NDC) as built-in dictionaries to prevent patient data from inadvertently leaving the organization
- Scan all servers and endpoint computers for PHI and PII data

The Code Green Networks’ TrueDLP™ solution is integrated with the Blue Coat® Systems ProxySG® appliances and McKesson Hospital Information Systems (HIS), providing organizations with a highly integrated healthcare data loss prevention solution. All traffic sent via the ProxySG or HIS can be inspected by the Code Green Content Inspection Appliance and blocked if necessary.

The comprehensive TrueDLP solution helps organizations protect patient data, prevent breaches from occurring, and ensure compliance with state and federal privacy regulations.

10-Day Data Loss Assessment

Code Green Networks offers a 10-day assessment service to demonstrate the power of TrueDLP for Healthcare and provide organizations with visibility into data loss occurrences that are taking place. During the assessment the TrueDLP™ solution is used to passively monitor network traffic and record data loss incidents. At the conclusion of the assessment a detailed report is provided summarizing observed incidents, how each loss occurred, and recommendations for corrective action.

Identify Unstructured Data – The next step in protecting patient data is identifying where any unstructured patient data is stored. This can take the form of documents containing a patient’s condition, kept on file shares, to patient records extracted from the Hospital Information System and stored in Sharepoint.

Determine Appropriate Policies – Once the data has been identified the next step is to determine what are the current polices for your environment. Are there rules around webmail and Web 2.0 (i.e. Facebook and Twitter)? What outgoing email should be encrypted? Are there rules around instant messaging?

Measure – Based on the information in steps 1-3 most Data Loss Prevention vendors will provide an assessment service using live data in your environment. This assessment will measure how well your current controls are protecting patient information; from there you can determine next steps.

Corporate Headquarters

Code Green Networks, Inc.
385 Moffett Park Drive, Suite 105
Sunnyvale, CA 94089
Phone: +1 (408) 716-4200
Fax: +1 (408) 716-4201
E-mail: info@codegreennetworks.com
www.codegreennetworks.com