



Preventing Data Loss in Healthcare Organizations

Protect your patient data against accidental or intentional data breaches

TrueDLP™ for Healthcare

Healthcare organizations have rich repositories of patient information and it is imperative that this data must be protected from both accidental and intentional disclosure. Gartner Research estimated more than 1 million cases of medical identity theft occurred in 2008 alone, and these numbers are likely to grow. With estimates suggesting that breaches cost companies \$202 per compromised patient record in 2008, the costs of even a small data loss incident can quickly escalate into the millions.

The types of data that healthcare organizations must protect against accidental or intentional disclosure are highly varied. Patient Personally Identifiable Information (PII), Protected Health Information (PHI), patient financial and insurance/payment information, and even sensitive documents such as physician peer reviews are often rich targets for medical identity theft. Additionally, Electronic Data Interchange (EDI) of patient data with business partners is subject to Health Insurance Portability and Accountability Act (HIPAA) regulations, and requires that all sensitive patient data be secured during communication.

Code Green's TrueDLP™ for Healthcare solution provides your IT staff with a sophisticated Data Loss Prevention (DLP) implementation that can detect, audit, block, and optionally encrypt sensitive data before it leaves your organization. From a single patient record inadvertently sent through an email over the Internet to large-scale patient database extract being copied to a USB flash drive on a desktop computer, TrueDLP for Healthcare offers the data protection that healthcare organizations urgently need.

Common Avenues for Data Exposure

While most data loss is inadvertent, resulting from human error or lack understanding of your organization's information disclosure policies, in many cases data loss is the result of a malicious effort to extract information. Both types of exposure share common paths that must be monitored and controlled:

Webmail communications - Webmail is commonly used by doctors and healthcare staff to communicate with patients and external partners, but unfortunately these communications are often insecure and result in patient data exposure.

Web 2.0 postings - MySpace, Facebook, Twitter and other web 2.0 applications are skyrocketing in popularity and have recently been the avenue for many data breaches. This path is also often used by data-stealing spyware/Trojan applications as a means of transporting sensitive data out of your organization.

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

FTP, IM, P2P 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.

Desktop USB and removable storage media - USB and other removable storage devices are ubiquitous, can hold large quantities of data, and are often difficult to control. Code Green's TrueDLP for Healthcare solution inspects data transfers on the desktop and can audit, block, or encrypt these transfers based on the specific content of the data.

Protects

- Patient Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Patient Financial Information
- Employee HR and Payroll Data
- Sensitive Organization Data, including Peer Reviews, Contracts, and strategic business plans

Monitors and Controls

- Email
- Webmail
- Web 2.0 Applications (e.g. MySpace and Facebook)
- File transfer applications such as FTP and P2P
- Desktop removable media

Discovers

- Sensitive data residing on end-points and servers

Get started with Code Green Networks

Visit our Web site at:

<http://www.codegreennetworks.com>

Unsecured partner communication - EDI 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. TrueDLP for Healthcare provides immediate audit visibility into these unsecured communications, and can block or encrypt the sensitive data being transmitted.

TrueDLP™ Data Loss Prevention

A data loss prevention solution must protect against sensitive data exposure yet must not interrupt the flow of business in your organization. The Code Green TrueDLP for Healthcare solution allows continued use of all communication channels while providing visibility and control over the data being transferred.

The Code Green TrueDLP for Healthcare solution accurately detects sensitive data by utilizing multiple sophisticated yet powerful content detection techniques. Content detection is based on actual patient data residing in an organization’s databases or file systems, offering far greater accuracy than simple pattern or keyword matching alone. For example, a policy rule for detecting Patient Identity Information (PII) loss might be written as: (Patient Name or Patient ID) AND Patient SSN

Rather than triggering on any 9-digit number, the policy is only triggered by the SSN of a specific patient, and only when detected in combination with the Patient Name or Patient ID. Accurate detection of actual patient data rather than generic pattern or keyword matching substantially improves accuracy and reduces false positives compared with traditional DLP solutions.

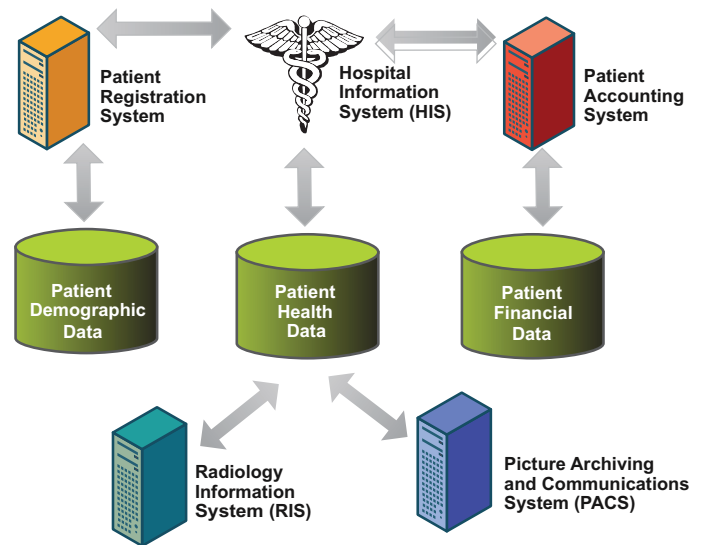
The TrueDLP for Healthcare solution scans databases containing sensitive patient data on a regularly scheduled basis and creates digital fingerprints of the content to use for data inspection. Fingerprints and not source data are stored on the appliance to ensure sensitive data is never at risk of compromise on the DLP appliance itself. When deployed in a healthcare IT environment, the solution is most often configured to import data from three primary databases:

- Patient demographic data maintained by the patient registration system—Contains significant PPII, including patient and insured names, addresses, IDs, and SSNs, insurance provider information, and employer information
- Patient health data contained in the hospital information system (HIS)— Contains PHI, including diagnostic and procedure codes
- Patient financial data contained in the patient accounting system – Contains patient credit card numbers, bank routing and account numbers, billing and collections information, and insurance reimbursement information.

For additional detection accuracy, the Code Green’s TrueDLP for Healthcare solution is pre-loaded with standard code sets, including HCPCS, ICD-9, LOINC®, SNOMED CT®, and NDC. The keyword and code identifiers in these code sets can be used in a policy to trigger a match. PHI almost always includes not just patient identity information but also one or more HIPAA treatment, diagnostic, procedure or observational codes.

“In the period from 2006-2007, more than 1.5 million content-rich records were exposed in hospital data breaches alone.”

HIMSS 2008 Report



Healthcare Specific Predefined Policies

Code Green's TrueDLP for Healthcare solution provides predefined policies and reports specifically designed to detect, prevent, and report on data loss in healthcare environments.

Pre-defined policies detect and control the following data:

- **PPII data** – Multiple policies detect, log, encrypt, and/or block PPII transmissions on the network or at the endpoint.
- **PHI data** – Multiple policies detect, log, encrypt, and/or block PHI. The policies are based on patient demographic data (Name or Patient ID) AND data from the HIS system or any of the HIPAA code sets.
- **Patient financial data** – Multiple policies detect, log, encrypt, and/or block patient financial data. Such information includes credit card numbers, bank routing or account numbers, billing and collections information, and insurance reimbursement information.
- **Unencrypted EDI** – Policies detect and report on any unencrypted HL7 and X12 messages, by source and destination. Unsecured partner EDI communications can be easily discovered and corrected.
- **HR and Payroll Data** – Employee data must also be protected from theft or disclosure. Policies detect and block HR and Payroll data leaked from internal HR and workforce management databases.

Data Loss Prevention across the Healthcare Enterprise

Code Green Networks TrueDLP for Healthcare solution is the first data loss prevention solution to provide network DLP, endpoint DLP, and discovery capabilities tailored to the needs of the healthcare industry.

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

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.

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.



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