



Data Loss Prevention for Healthcare

Healthcare organizations today possess and manage a tremendous amount of electronically stored personally identifiable and sensitive information. Ensuring the security of these critical assets is imperative for healthcare organizations to demonstrate compliance and protect their brand name and reputation. Even more troublesome for healthcare organizations is the rapid rise in medical identity theft—now the fastest growing form of identity theft—costing healthcare organizations millions of dollars each year. According to James Quiggle, from The Coalition Against Fraud, the most common form of medical identity theft is insiders at clinics, hospitals, and other facilities stealing lists of patients and their information and reselling them for huge profits.

Once your strategy is finalized and you are ready to implement a solution to combat data loss, trust Code Green Networks. Code Green Networks provides healthcare organizations with affordable and easy-to-manage solutions for protecting confidential data including: Electronic Health Records (EHRs), Individually Identifiable Health Information, and payment card holder data. In addition, Code Green Networks solutions for healthcare safeguard against the unauthorized transmission of sensitive business documents and intellectual property including policies & procedures for billing and treatments, peer reviews, corporate financials, and legal documents.

Common Concerns Among Healthcare Organizations

- Unauthorized individuals are viewing and/or taking files that include protected health information (PHI).
- Doctors are sending sensitive files to their Webmail account, so they can access the information from a home/remote computer.
- Physicians are sending sensitive documents, such as peer reviews and policy/procedure details for billing and treatments, out to external recipients.

Products/Services

From medical identity threats to complying with the Red Flags Rule and state/federal regulations, Code Green Networks offers market-leading data loss prevention solutions that help healthcare organizations protect PHI and other sensitive data, thereby mitigating the risk of unauthorized disclosure of confidential information. Code Green Networks solutions are designed from the ground up to be affordable and easy-to-manage, with typical installations taking less than a day.

Content Inspection Appliances (CI-1500/CI-750)

Code Green's Content Inspection Appliances enable healthcare organizations, of any size, to effectively monitor, enforce and audit the loss of patient/confidential data across all popular Internet communications channels - including email (SMTP), Web (HTTP), Secure Web (HTTPS), and File Transfer Protocol (FTP). Online applications and services such as WebMail, Social Networks, Blogs and Wikis are fully inspected for sensitive data and all transactions/postings are blocked if necessary.

Key Benefits

- Compliance with regulations such as HIPAA, Red Flags Rule, PCI, and state/federal privacy regulations
- Automated email encryption utilizing policy-driven healthcare data classification and filtering
- Unobtrusive enforcement of data loss prevention policies across all popular Internet communication channels
- Healthcare code sets (e.g. HCPCS, ICD-9, LOINC, and NDC) as built-in dictionaries
- Inclusive data logs of confidential data copied, sent, or downloaded

Features

- Affordable and easy-to-manage
- Monitors and enforce electronic communications
- Integrated email encryption
- Predefined policy templates
- Quick deployment

Get started with Code Green Networks

Visit our Web site at:

<http://www.codegreennetworks.com>

Content Inspection Agent (CI Agent)

The Code Green Networks Content Inspection Agent (CI Agent) provides total visibility and complete control over sensitive information residing on servers, laptops, and removable media. The CI Agent provides healthcare organizations both Endpoint DLP and Discovery.

- The Endpoint DLP component provides both device level control and content aware inspection, allowing flexible policy-based enforcement. Detailed activity logging provides audit history information necessary to demonstrate compliance. Offline policy enforcement ensures protection for laptops and other devices even when disconnected from the network.
- The Discovery component locates and identifies sensitive data at rest on endpoints and servers across the network, providing visibility and audit reporting of potentially unsecured information.

TrueDLP Detection Accuracy for Healthcare

Through proprietary fingerprinting technology Code Green Networks is able to recognize and register a wide variety of both structured (fields in databases or columns in spreadsheets) and unstructured data (document formats such as Microsoft Office, source code and PDF files) eliminating the high false positives and false negatives to ensure the capture of incidents specific and relevant to your organization.

In addition the Code Green Networks healthcare solution includes healthcare code sets (e.g. HCPCS, ICD-9, LOINC, and NDC) as built-in dictionaries, enabling data loss prevention policies that immediately detect and protect sensitive protected health information (PHI) whether in network transmissions, in use on the desktop, or stored in files across the enterprise.

Partnerships for Success

Code Green Networks has forged solid partnerships with leading technology companies to further enhance and expand its product offerings. By leveraging these complementary solutions within our products, we continue to deliver what businesses need to protect their confidential information.

ZixCorp - As the largest hosted email encryption service provider, ZixCorp protects millions of email addresses including those of some of the nation's most influential healthcare institutions. By integrating Code Green Networks Data Loss Prevention solution with ZixCorp's email encryption, organizations can ensure data protection across all network channels, including WebMail, FTP, blogs, and popular social networking sites, not just SMTP-based email. Integrating data loss prevention and email encryption provides the best of both worlds – powerful and accurate data loss prevention across all network channels together with enhanced policy based email encryption to secure sensitive communication.

Blue Coat Systems - Blue Coat solutions provide a layered approach for inbound and outbound Internet gateway protection from spyware, malware, mobile malicious code, viruses, trojans, botnets, phishing and Web 2.0 threats. Together Code Green Networks and Blue Coat offer organizations a highly integrated, standardsbased data loss prevention solution for monitoring and controlling Web and FTP traffic, including control over SSL-encrypted sessions.

Blue Coat ProxySG appliances share information and access to Web and FTP sessions with Code Green Content Inspection Appliances using an enterprise-class implementation of the Internet Content Adaptation Protocol (ICAP). The Content Inspection Appliances inspect the traffic for sensitive content and apply the appropriate DLP policy. Based on policy, the Content Inspection Appliance instructs the Blue Coat ProxySG to allow or block the session.

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.



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