

# Data Loss Prevention for Healthcare

## The Increasing Challenge for Healthcare Organizations

Healthcare organizations today manage enormous amounts of sensitive information in their enterprises. Most important of all the various types of sensitive information they process are the thousands of patient records that stream across their networks on a daily basis that include: personal health information, personally identifiable information and even payment cardholder data.

Data breaches, either accidental or through malicious intent, have become commonplace in the connected business environment and the growth of personal and corporate online communications tools available today create even more challenges for healthcare organizations trying to secure protected health information (PHI) and their own intellectual property.

The average cost of a data breach now exceeds \$100 per record and over \$4 million per incident – with estimates that 75% of the \$200 billion in measured annual security losses come from within organizations due to unauthorized and often inadvertent disclosure of proprietary business or customer information and intellectual property. This is a considerable cost and challenge for any industry.



### Benefits

- Secure patient protected health information (PHI)
- Protect customers' personally identifiable information
- Demonstrate compliance with HIPAA, PCI-DSS and state data privacy laws
- Secure communications with doctors, pharmacies, insurance companies and other business partners
- Safeguard confidential business information

### Features

- Affordable & Easy-to-Manage
- Monitors & Enforce Electronic Communications
- Integrated Email Encryption
- Predefined Policy Templates
- Quick Deployment

What Types of Information Does Your Organization Handle? Demonstrate Compliance	
<b>Personal Health Information</b>	name, date of birth, diagnoses, medical procedures, point/date of service, medical record numbers, insurance benefit numbers, etc.
<b>Personally Identifiable Information</b>	social security numbers, driver's license numbers, account information
<b>Payment Cardholder Data</b>	primary account numbers, names, service codes, expiration dates, etc.
<b>Company Intellectual Property</b>	operational plans, sales & marketing plans, corporate financials, contracts, M&A, legal documents, etc.

## Securing PHI & Demonstrating Compliance

For healthcare organizations, assuring the security of PHI and the information assets it resides on is crucial for demonstrating regulatory compliance and protecting their brand and reputation.

First and foremost, all organizations that handle PHI are required to comply with the Security Rule under the Health Insurance Portability and Accountability Act (HIPAA) which provides specific safeguards for the secure handling, management and transmission of electronic protected health information (EPHI).

Healthcare organizations today may also be required to demonstrate compliance with ever-increasing state privacy laws (such as California's SB 1386) and Federal Trade Commission (FTC) guidelines that specifically outline how personal information should be handled and the notifications and penalties in the event of a breach of this sensitive data. If credit card transactions are handled by the healthcare organization, they may also be required to comply with the Payment Card Industry Data Security Standards (PCI-DSS) for securing and handling of customer data.

### Get Started

For more information on Code Green Networks solutions, visit our Web site at:  
<http://www.codegreennetworks.com>

The risk factor for a healthcare organization runs deeper than simple compliance. Failure to take appropriate measures to secure PHI and safeguard their own intellectual property can result in loss of revenue, financial penalties and irreparable harm to an organization's image, brand and customer loyalty.

Small and medium-sized healthcare organizations today face the same challenges and risks as larger organizations in seeking to secure PHI and intellectual property while complying with this growing regulatory environment. While the risks and requirements are the same, these smaller organizations generally have fewer resources to tackle the challenges. That is where the need for affordable, easy-to-manage, yet enterprise class data loss prevention solutions is the greatest.

Regulation	Issue for Healthcare Organizations
<b>Health Insurance Portability and Accountability Act (HIPAA)</b>	The Health Insurance Portability and Accountability Act (HIPAA) requires organizations entrusted with Protected Health Information (PHI) to protect this data against deliberate or inadvertent misuse or disclosure. More specifically for electronic protected health information (EPHI), organizations must meet specific safeguards for the secure handling, management and transmission of this type of data.
<b>Payment Card Industry (PCI)</b>	The Payment Card Industry (PCI) group was formed in 2004 to create common industry security requirements acceptable to all cardholder associations such as Visa, and MasterCard. The standards define how cardholder and card authentication data must be stored, managed and processed to keep it secure.
<b>State Data Privacy Laws</b>	Since the passing of California's security breach notification law (CA SB 1386) in July 2003, more than 35 states have enacted laws that specifically protect consumer privacy by requiring organizations to safeguard data collected from consumers who reside in those states and in circumstances where private data has been potentially exposed, the organization must notify consumers who are affected.
<b>Federal Trade Commission (FTC) Guidelines for Protecting Personal Information</b>	Guidelines published by the Federal Trade Commission (FTC) in April 2007 provide significant detail on what the FTC considers to be reasonable and appropriate steps for businesses to protect the privacy of electronic personal information they maintain ( <a href="http://www.ftc.gov/infosecurity">www.ftc.gov/infosecurity</a> ). These guidelines point to the need for data loss prevention solutions, automated email encryption for messages containing sensitive information, and ultimately form the basis for what is considered best practice for protecting personal information.

“Small and medium-sized healthcare organizations face the same challenges as larger organizations in seeking to secure PHI...”

## The Evolving Regulatory Environment

Demonstrating compliance with just the existing regulatory environment – including HIPAA, PCI, CA SB 1386 and others – is a challenge for healthcare organizations today. But with so much attention being paid to protecting consumer's privacy and personal information, the regulatory environment continues, and will continue, to evolve at both a state and Federal level – and with it the challenges of demonstrating compliance and keeping up with these changes for all types of organizations will only increase.

## California's Recent Amendments to Breach Notification

California continues to drive the agenda in terms of security breach notification legislation. California's security breach notification law, CA SB 1386, was the nation's first and today more than 35 states have similar laws. California's law requires disclosure of any security breaches involving 'personal information,' which the law defined as an individual's name in addition to his or her Social Security number; driver's license number or California identification card number; or an account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

In a continuing effort to protect consumer privacy, lawmakers in California approved legislation that went into effect on January 1, 2008 that amends the state's security breach notification law to add two new categories of information to the definition of personal information: medical information and health insurance information.

The impact of these two new categories is not limited to healthcare providers, but may affect any employer or other entity with computerized employee benefits or other health information.

While this legislation today only applies to those organizations doing business in California, it is very likely these amendments will work their way across the country and around the world in the same way SB 1386 has changed the US and international landscape for mandating security breach notifications.

Any way you look at it, these amendments are a clear signal to healthcare organizations and businesses of all types that the regulatory environment will continue to evolve and expand to further protect consumer privacy and the best course of action for any organization that handles or managed personal information should be to take aggressive steps to secure that data or risk public exposure and damage to brand and reputation.

## New Communications Channels & Risks to Data

The amount and types of communications channels available today continues to expand and each serves as a potential new vector for data loss – either accidental or malicious. From WebMail to Blogs and Wikis, the range of online collaboration and communication tools continues to expand every day and security professionals are continually challenged to keep up with this growth and continue to apply policies to them.

In particular, the use of consumer WebMail services, such as Google's Gmail, Yahoo! Mail, Hotmail and others, represent ways in which standard security controls and data policies can be bypassed and compliance undermined.

The majority of healthcare organizations today have little to no control over how consumer WebMail services and online collaboration tools are used on, or understand what data or information may be unknowingly leaving, their networks. Some organizations have even taken steps to shut down access completely to consumer WebMail services – not allowing staff, doctors or other personnel to send or receive WebMail messages while on the organization's network. For most organizations this is not a realistic solution.

Organizations of all types, but in particular those that manage such vast amounts of personal information like healthcare providers, must be able to proactively identify, audit and apply policy to sensitive information across all potential leak points. Outright blocking of communications channels is not a realistic solution to the problem. By identifying

**“...the regulatory environment will continue to evolve and expand to further protect consumer privacy...”**

sensitive information, barriers can be put in place and all communications monitored without having to interfere with normal business processes and activity. Doctors and staff should be able to access their WebMail accounts without security managers fearing policies will be violated and no audit trail or proactive measures taking hold.

In addition, protection for specialized types of information such as drug interaction issues, HIV lists, medical records, financial plans and other types need to be protected. It is far better to erect a barrier around these types of confidential information today and keep them from leaving the network instead of having to try to get it back once it does.

## Affordable DLP for Healthcare

Code Green Networks provides healthcare organizations such as hospitals, doctors' offices, pharmacies and health services organizations with affordable and easy-to-manage solutions for protecting confidential data such as personal health information, personally identifiable information and payment cardholder data. In addition, Code Green Networks solutions safeguard sensitive business information and intellectual property including corporate financials, contracts, legal documents and sales and marketing plans.

With Code Green Networks, healthcare organizations can easily and affordably secure PHI and demonstrate regulatory compliance.

Here are just some of the benefits Code Green Networks provides for healthcare organizations.

### Affordable & Easy to Manage

Code Green Networks solutions provide enterprise class data loss prevention capabilities in an affordable and easy-to-manage package. Solutions are designed specifically for small and medium-sized healthcare organizations and can typically be deployed in one business day or less.

### Secure Protected Health Information

Code Green Networks protects any type of data or protected health information (PHI) stored in databases, or other structured files using proprietary Data Element Fingerprinting technology. Once the content is registered, it is protected in line with policies across all network traffic — and violations handled with established workflow and logged for future auditing purposes.

### Demonstrate Compliance

For healthcare organizations seeking to demonstrate compliance with HIPAA, Federal or state data privacy and notification laws (such as CA SB 1386) or even PCI-DSS, Code Green Networks provides predefined policy templates that enable quick set up and easy configuration.

### Automatically Encrypt Email Messages

Healthcare organizations can effectively automate the process of encrypting confidential information transmitted in electronic communications through Code Green Networks' integrated, policy-based email encryption technology. Messages containing PHI or other confidential information can be automatically identified and encrypted based on a policy action and logged for future auditing and reporting purposes. And no additional hardware or software is required.

**“...in particular the use of consumer WebMail services represent ways in which standard security controls and data policies can be bypassed and compliance undermined.”**

## Apply Security Policies to WebMail

Code Green Networks enables organizations to easily define policies that not only inspect Internet traffic across all major online communications channels, but consumer WebMail as well.

## Out-of-the-Box Support for Detection of Clinical Document Architecture (CDA)

The CDA, which was until recently known as the Patient Record Architecture (PRA), provides an exchange model for clinical documents (such as discharge summaries and progress notes) — and brings the healthcare industry closer to the realization of an electronic medical record. Code Green Networks includes default policies that recognize CDA documents and attachments in network traffic, allowing their transmission to be managed appropriately (e.g. logged, blocked, encrypted).

## Safeguard Intellectual Property

To safeguard confidential business information such as financial documents, sales and marketing plans or other intellectual property, Code Green Networks proprietary Deep Content Fingerprinting technology registers and detects unstructured content across more than 400 file types and in any language. Content is monitored, inspected and policies are applied to safeguard its transmission and logged for future auditing and reporting purposes.

## Predefined Policy Templates

Code Green Networks provides a complete, customizable set of pre-built policy templates designed to allow content authorities to quickly and easily define and roll out policies that meet their organization's requirements for compliance or best practices.

## 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.

For more information about Code Green Networks, visit <http://www.codegreennetworks.com>



## Corporate Headquarters

Code Green Networks, Inc.  
3975 Freedom Circle, Suite 900  
Santa Clara, CA 95054

Phone: +1 (408) 213-2300

Fax: +1 (408) 213-2301

E-mail: [info@codegreennetworks.com](mailto:info@codegreennetworks.com)