White Paper

# Data Loss Prevention Best Practices for Healthcare

**The perils of data loss**

intel Security

**This white paper is co-authored with Siemens Healthcare**

# Table of Contents

By virtue of an ever-changing web of regulations that span federal, state, and local jurisdictions, healthcare organizations are required to safeguard patient data, including ePHI (Electronic Protected Health Information). On September 23, 2013, all healthcare organizations were obligated by law to comply with the HITECH Omnibus Final Rule, which outlines requirements for encrypting and protecting ePHI data. In addition, healthcare organizations that suffer a security breach, lose ePHI data, or fail to recover quickly enough following a disaster may be investigated by the Office of Civil Rights (OCR) and could face fines in the millions of dollars.

A monumental challenge for healthcare organizations is support of the accelerating demands placed on healthcare professionals to deliver higher quality care at a faster pace across multiple organizations, while consistently assuring secure data handling. Simply building firewalls at the network perimeters is ineffective against stealthy attacks and advanced persistent threats. Cybercriminals can enter an organization's network, exploit weak points, and breach data for weeks or months before detection. From 2010 to 2013, cybercrime attacks have increased from 20% to 33%.1 Employing sound data loss prevention practices and processes helps ensure the safe handling of data, provides the flexible environment required by clinical staff, and helps organizations pass rigorous OCR audits easily and reliably.

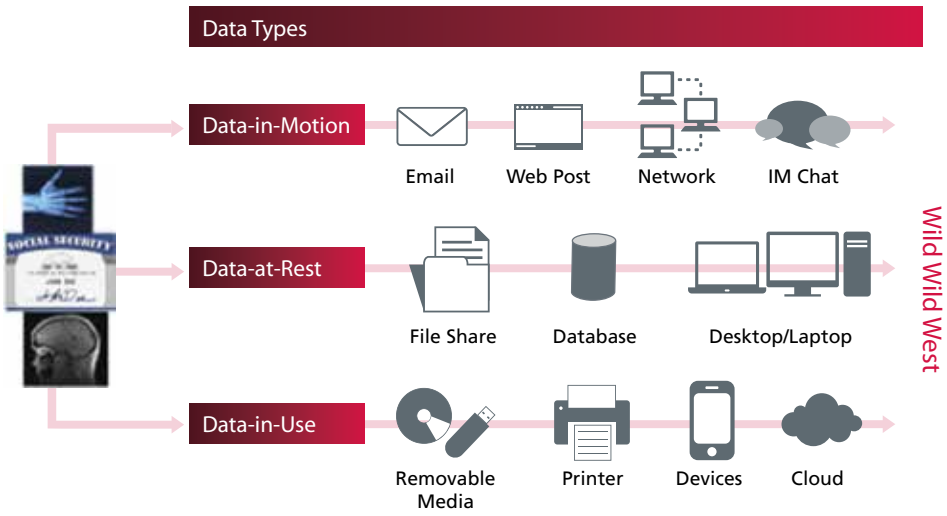


**Figure 1.** Various ePHI data access points that warrant protection.

## First Steps to Data Loss Prevention

### You Cannot Protect What You Don't Know

Within healthcare organizations, data is constantly being created, replicated, modified, moved around, and disseminated. Internal data sprawl has become an issue because the IT department responsible for security and compliance doesn't fully know what data it really needs to protect or its value to the organization. IT doesn't know where all the ePHI data is stored, who owns it, how it's being used, or who has access to it. You cannot protect what you don't know you have, where it's located, or who has access to it.

**Better Visibility Via Monitoring Technology**

At the early stage of implementing a data loss prevention (DLP) solution, it's critical to implement a monitoring technology that can gather, track, and report on the data in motion across your entire network in real time. Such tools help you learn what and how information travels inside and out of your organizations, and the data gathered will help you identify potential risks and support your planning for a better data security posture. Understanding your data makes all the difference, as it enables you to build the right policies to protect the right data for the right cost—without trial and error.

**Faster Data Discovery and Remediation Via Classification**

Sensitive data such as ePHI can be scattered across thousands of servers, in millions of files, and can be mixed with a significant amount of unknown content. One option is to run an extensive discovery scan, which opens every single file on all the servers. This approach can be extremely time-consuming, and generates a huge list of potential security violations and false positives which take time and money to investigate.

A better approach is to classify and categorize files on servers before a full-on discovery scan. For example, a quicker inventory scan can be done based only on the file's metadata (file owner, file type, file size, file owner, share name, count, and other information). The inventory step can be accomplished quickly because only the metadata of the files are being analyzed, not the entire file, which is the computationally expensive part. Once the files are categorized, DLP policies can then be applied to perform analytics on the classified content. As a result, remediation workflow (for example, server 1 has 10 Microsoft Excel files containing ePHI data that needs attention) can be more streamlined. It's important to deploy a data discovery and remediation solution with a built-in data classification engine that can provide a scalable and rapid way to classify your data and reduce risk with low false positives.

In many hospitals, the IT department is neither aware nor actively engaged in managing niche departmental systems that are often repositories of ePHI and/or other sensitive information. A scalable and efficient discovery process can aid the IT department in locating, identifying, and classifying data in isolated ancillary systems. Furthermore, this discovery effort can segue into better platform management, ensuring that critical tasks, such as backup, patching, privacy auditing, and environmental security concerns are adequately addressed.

## DLP Is a Program and a Process

Most organizations think of DLP as purely a technical problem. They assume that if they deploy DLP technology, it will find the issues. The reality is that deploying DLP systems is part of a broader data protection program. Having the best DLP detection technologies in the mix of broken business processes will not prevent sensitive information from finding its way out of the organization in unanticipated and uncontrolled ways.

**Data Protection Awareness Program**

While you are implementing a DLP solution, adoption of an employee data protection education and awareness program is recommended. Leverage this program to modify employee behavior when it comes to handling ePHI.

Generally, a hospital workforce does not maintain heightened security awareness, leading to misuse and potential for breach of ePHI. Making it easy for the workforce to do the right thing leads to far greater success than policing unaccustomed activity. For example, prohibiting or requiring attestation when attempting to transfer ePHI onto a mobile device or through a web application is not much different than enforcing the closed-loop medication administration to better ensure patient safety.

**Governance**
It is important that IT maintains the DLP technology platform and its configuration. However, business units should be responsible for deciding the business rules and resolution of data loss (breach) events. Even before deciding or implementing any DLP technology solution, key stakeholders from the business units, compliance, and privacy teams, and the CIO have to come to an agreement on clearly defined roles and responsibilities (who has access and authorization to view and act on incidents, what is the data governance communication plan, and benchmark metrics).

## Tailor DLP Policies to Your Environment

According to the latest Verizon Data Breach Report,2 cybercriminals install malware to collect and exfiltrate (export) data. While many industry experts talk about advanced threat detections and anti-evasion techniques, such as intrusion prevention systems (IPS) and next-generation firewall, it is not about "if" the malware gets in, it's more about "when" the malware gets in. What do you do? DLP is your last inline layer of defense.

Any healthcare DLP technology solution should include the following features and functionality tailored to the environment:

- DLP policy templates specifically designed for healthcare organizations.
- Customized protocol handlers to identify HL7 v2, HL7 v3, or e-PHI transmitted over X12.
- Specialized connectors with major vendors' application portfolios: Siemens, Cerner, EPIC, Meditech, GE Health Systems, and McKesson.
- Customized reporting based on content sources and violations mapped to the content source for refinement and reduction of false positives relative to healthcare EMR systems.
- Specific healthcare code sets (HCPCS, ICD-9, ICD-10, LOINC, and NDC) as built-in lexicon dictionaries to prevent patient data from inadvertently leaving the organization.
- Integration from the endpoints to the network and through the gateway (email/web).

A world-class DLP solution should not only be quick to deploy with built-in templates, but also help you understand your data, identify broken business processes, and give you flexible tools to protect ePHI and other sensitive files completely and quickly. It can assist you with achieving and maintaining regulatory compliance, give you oversight and control, and help you maintain the trust of your auditors, practitioners, and patients.

## DLP that Saves You Time

You need a DLP technology solution that is quick to deploy with easy day-to-day management. Look for a solution that can offer tightly integrated endpoint and network components to ensure that your sensitive data is protected—from the USB drive to the network perimeter and beyond. Having a single console that can set policies and manage incidents and violations with an automated workflow can help save you time and reduce cost. And don't forget the power of your users. Choose a DLP endpoint solution that offers user remediation consoles and user tagging to help alleviate administrative burdens and promote data protection awareness amongst employees.

## Summary

The financial, legal, and public relations risks for healthcare organizations that experience ePHI breaches continues to mount. Employing a sound DLP strategy is critical in the current healthcare environment. Understanding what data you own and who has access to it is a paramount primary step to better control of ePHI. Properly classifying data and utilizing monitoring technology to continuously track data location and movement is essential.

## McAfee Data Loss Prevention

McAfee® Data Loss Prevention is quick to deploy, flexible to control, easy to manage, and can help you better understand the data that you are trying to protect. This comprehensive solution safeguards sensitive data and ensures compliance by protecting ePHI data wherever it lives: on premises, in the cloud, or on endpoints. Unique, non-invasive technology discovers, tracks, and classifies data no matter where it resides or what format it is in, giving you rich insight and delivering fast, effective protection.

## About Siemens

The Siemens Healthcare Sector is one of the world's largest suppliers to the healthcare industry and a trendsetter in medical imaging, laboratory diagnostics, medical information technology and hearing aids. Siemens offers its customers products and solutions for the entire range of patient care from a single source—from prevention and early detection to diagnosis and on to treatment and aftercare. Siemens Healthcare offers healthcare domain expertise and a broad set of services to cover all of a healthcare organization's security and privacy mitigation services needs.

## About McAfee

McAfee, part of Intel Security and a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence network, McAfee is relentlessly focused on keeping its customers safe. **http://www.mcafee.com**

1. *Global Threat Trends*; [cited 2014 Jan 10]; Available from: **http://www.eset.com/us/resources/threat-trends/Global_Threat_Trends_June_2013.pdf**.
2. *2014 Data Breach Investigations Report*, Verizon, April 2014.

**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com