SOLUTION SHEET

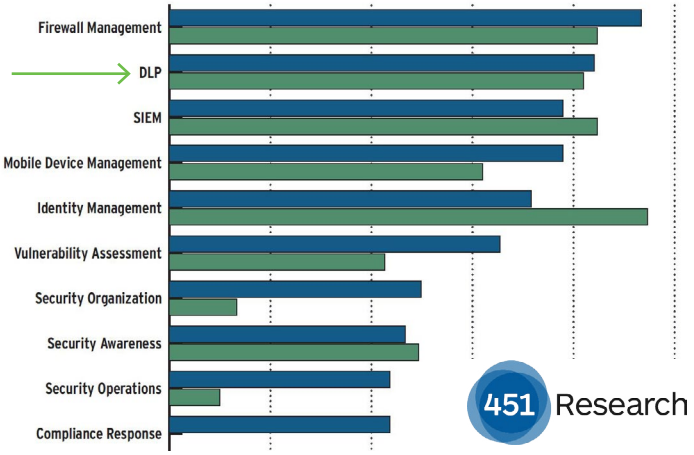
DIGITALGUARDIAN®
For Healthcare

WHY DATA LOSS PREVENTION FOR HEALTHCARE SYSTEMS

DLP CAN PROVIDE A SIMPLE COMPLIANCE FRAMEWORK TO PREVENT THE LOSS OF PHI

Data Loss Prevention is a powerful tool to ensure compliance with regulations such as the HIPAA Security Rule, Joint Commission, and state privacy regulations. It can help you **analyze** the risks to PHI, **educate** employees on security polices in real-time and **assess** areas for improvement. According to a recent 451 Research survey of IT professionals, DLP is one of their top priorities in 2015-2016.

INFORMATION SECURITY PROJECTS - TOP CATEGORIES



1 ANALYZE POTENTIAL RISKS TO ELECTRONIC PHI

Protection starts with understanding your risks. The best DLP tools provide a number of mechanisms to analyze risks to PHI per the HIPAA Security Rule and limit PHI access to the "Minimum Necessary".

- Discover PHI stored on laptops, workstations, and servers that are unencrypted
- Measure PHI being emailed out of your organization
- Detect PHI being transferred out of your organization in unencrypted FTP
- Audit PHI being copied to USB devices or burned to CDs or DVDs
- Track and control PHI in, or being uploaded to, the cloud

2 EDUCATE CARE PROVIDERS ON SECURITY POLICIES — IN REAL TIME

Employees are your biggest risk. Data Loss Prevention tools prevent user actions that put your organization at risk and educate users in real time on the appropriate handling of PHI.

- Prompt a user for justification when PHI is copied to removable media
- Notify a user when a file containing PHI is attached to an email leaving your organization
- Notify an administrator when a file containing PHI is copied to an unprotected share
- Move a potentially sensitive file trying to be uploaded to the cloud to a protected folder

3 PERIODICALLY ASSESS SECURITY POLICIES

You can't improve what you don't measure. Data Loss Prevention tools provide a mechanism to continuously assess security policies and procedures

- Inspect every email and web transaction for the presence of PHI
- Measure effectiveness of other controls by monitoring where PHI is moved once it leaves your central EHR system
- Get daily, weekly, and monthly reports measuring incidents of interest and potential loss trends

DIGITALGUARDIAN®

For more information, visit
www.digitalguardian.com

A DIFFERENT APPROACH

Digital Guardian believes that data protection products offered to address regulatory compliance are often needlessly complex to implement and difficult to manage, leading to unplanned costs and delays that result in diminished benefits to the organization. Digital Guardian has taken a different approach. Our technology for identifying and controlling compliance data such as PHI is the industry's most accurate. By focusing on protecting PII/PHI, Digital Guardian delivers a compliance solution that is recognized as the easiest to deploy and manage, with the absolutely lowest false positive rates.

DLP ON THE NETWORK, ENDPOINTS AND IN THE CLOUD

Digital Guardian for Compliance enables hospitals to effectively discover, monitor, control, and PHI, whether on the network, in use on desktops or laptops, at rest on end-user devices and network servers - or stored in the cloud.

Our Cloud Data Protection allows hospitals to **adopt cloud storage** while maintaining the visibility and control needed to comply with privacy and data security regulations.

ENTERPRISE DLP IN 30 MINUTES OR LESS PER DAY

Digital Guardian's simple architecture combines:

- Content Inspection
- Policy creation/management
- Email encryption

No dedicated resources required to manage.

Plus Digital Guardian for Compliance is also available as a managed service.

"Implementation is greatly simplified... with average deployment times much shorter than other DLP products. Implementations can often be completed in a single day, with only minimal policy tuning required thereafter."

- Data Loss Prevention Leading Vendors Review, DLP Experts, 2016

DLPX DATA LOSS PREVENTION EXPERTS

THE MOST ACCURATE PHI DETECTION

Our Database Record Matching fingerprinting technology is the industry's most accurate for identifying and controlling PHI. By focusing on protecting PHI, we provide hospitals with the absolutely **lowest false positive rate** of any technology available.

For example, 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.

This allows healthcare IT teams to focus on the real risks.

"Within literally minutes of the appliance being plugged in, we started collecting data. Once we saw items that could become major issues for us, we were able to remediate potential problems right away."

- Steve Scott, Information Security Manager, Saint Charles Health System

St. Charles HEALTH SYSTEM

DIGITALGUARDIAN®

For more information, visit
www.digitalguardian.com

HOW DIGITAL GUARDIAN FOR COMPLIANCE MEETS HIPAA STATUTES

HIPAA STATUTE	HOW DIGITAL GUARDIAN HELPS
Statute 164-306, Security standards Requires a Covered Entity to ensure the confidentiality, integrity, and availability of all electronic protected health information the Covered Entity creates, receives, maintains, or transmits.	Our complete solution helps with the confidentiality portion of this safeguard by : • Detecting and preventing email containing PHI from being transmitted to the internet • Detecting and preventing network transmissions containing PHI from leaving your network (including email or access to webmail providers such as Gmail) • Detecting and securing any unencrypted PHI found on workstations, laptops or network file shares with inadequate controls • Detecting and preventing PHI from being copied to USB devices (or burned to DVD/CD) • Detecting and preventing PHI from being uploaded to cloud storage
Statute 164-308, Administrative safeguards, section A, Risk Analysis Requires a Covered Entity to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the Covered Entity.	Our complete solution will continuously assess potential confidentiality risks to PHI by providing the following capabilities: • Continuously scan all network traffic (including email, webmail and other traffic) destined for the internet to identify and block potential external transmission of unencrypted PHI • Periodically assess unencrypted PHI on workstations, laptops, and file systems to determine if any data is being stored in locations including the cloud without proper controls • Monitor all data copied to USB and prevent any PHI from being copied without adequate encryption controls
Statute 164.312, Technical Safeguards Requires a Covered Entity, in accordance with §164.306, implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	Our data discovery solution addresses this safeguard by discovering unencrypted PHI on systems with inadequate controls. The discovery process scans File Shares, Workstations, SharePoint Servers and Databases for confidential information Our endpoint compliance solution addresses this safeguard by detecting and blocking or encrpyting PHI about to be written to USB, CD or DVD.
Statute 164-312 (e)(1), Technical safeguards: Transmission Security Requires a Covered Entity to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Our Network DLP solution detects unencrypted PHI leaving your organization's network for the internet. This capability has specific mechanisms to: • Detect and prevent PHI from being sent via email • Detect and prevent PHI transmission over HTTP/ HTTPS • Audit that patient data is not being sent via any other protocol

DIGITALGUARDIAN®

For more information, visit
www.digitalguardian.com

DIGITAL GUARDIAN — PURPOSE-BUILT FOR HEALTHCARE SYSTEMS

FULLY INTEGRATED WITH THE LEADING EHRs

Our solution accurately detects sensitive data by utilizing multiple sophisticated yet powerful content detection techniques. Content detection is based on actual patient data residing in your EHR system. Digital Guardian for healthcare is integrated and tested with the leading EHRs.

Allscripts™ Cerner™ Epic

Centricity MEDITECH Medical Information Technology, Inc. McKESSON Empowering Healthcare

HEALTHCARE SPECIFIC PREDEFINED POLICIES

Our solution provides predefined policies and reports specifically designed to detect, prevent, and report on data loss in healthcare environments. These pre-defined polices detect and control the following data:

- **PHI data –** Multiple polices 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.

A TRUSTED PARTNER

DIGITAL GUARDIAN IS SUCCESSFULLY DEPLOYED IN MORE THAN 100+ HEALTHCARE SYSTEMS

ABOUT DIGITAL GUARDIAN

Digital Guardian is the only data aware security platform designed to stop data theft. The Digital Guardian platform performs across traditional endpoints, mobile devices and cloud applications to make it easier to see and stop all threats to sensitive data. For more than 10 years we've enabled data-rich organizations to protect their most valuable assets with an on premise deployment or an outsourced managed security program (MSP). Our unique data awareness and transformative endpoint visibility, combined with behavioral threat detection and response, let you protect data without slowing the pace of your business.

SHARE