FORTRA™

SOLUTION BRIEF (DIGITAL GUARDIAN)

Digital Guardian for Healthcare

Why Threat Aware Data Protection For Healthcare

As the demand for patient data grows, so does the need for data security. According to PwC's recent information security survey, the largest healthcare breaches in history were reported over the past year. This has lead payers and providers to rank data loss prevention their top security challenge.

All healthcare organizations must comply with the stringent regulatory requirements of HIPAA and HITECH to safeguard patients' Protected Health Information (PHI), Personally Identifiable Information (PII).

Complicating these compliance efforts is the growing trend of migrating patient data to cloud storage and hosted applications such as Health Information Exchange systems. The cloud lowers costs and improves efficiency, but widens the attack surface for data breaches.

$363

Average cost of a lost/ stolen data record for healthcare companies

$154

Average cost of a lost/ stolen data record for other organizations

136% HIGHER

than the global average cost of a non-healthcare related data breach per lost or stolen record

(sources: 2016 Verizon, Ponemon Institute, PwC)

Key Challenges

Healthcare payers and providers must protect their data from a range of threats:

Insider Threats

Current or former employees, either by malice or mistake, leak PHI to egress channels such as email, media, and mobile devices. 55% of all attacks originate with insiders, many of whom fall victim to email phishing attacks.

Ransomware

Attackers hold patient data hostage, forcing suspension of critical services and impeding communications until payment is extorted. This epidemic has hit hospitals particularly hard, and grew to 4,000 attacks per day in Q1 2016.

Third Party Infiltration

Cyber criminals can compromise trusted partner providers, maintenance contractors and clients who lack adequate security controls -- gaining backdoor access to sensitive health data. Such attacks increased 56% in a single year.

How Digital Guardian Can Help

Understand: What Data To Protect

Fortra™'s Digital Guardian® with its deepest visibility into data, user and system events, can identify and tag sensitive data in real-time even before you develop formal policies. We accurately identify PHI using our Database Record Matching fingerprinting technology. 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.

Understand: When Data Is At Risk

The Digital Guardian platform harnesses our deep visibility and real-time analytics to discover, monitor and control structured data such as PHI and PII as effectively as unstructured data such as clinical research data. Our solution monitors enterprise data wherever it lives and wherever it is shared – across networks, storage, endpoints, or in the cloud – performing equally across Windows, Apple or Linux platforms.

Enforce And Educate: Flexible & Automated Controls

Our behavior-based rules automatically prompt users to prevent actions that violate policies and put data at risk. Users are educated in real-time with positive reinforcement on the appropriate handling of regulated data via display prompts that request justification. Illegal downloads or exfiltration can be blocked or contained before the data is gone.

Digital Guardian Protects Both Your Structured And Unstructured Data

Hospitals

- Personal Health Information (PHI)
- Patient Financial Information

Healthcare IT

- Patient care data
- Personal Health Information (PHI)
- Personally Identifiable Information (PII)

Healthcare Analytics

- Claims & cost data
- Unstructured data such as R&D data, clinical data, patient behavior & sentiment data

Benefits Management & Insurance

- Personal Health Information (PHI)
- Claims data
- Patient Care Data

Meeting Hipaa Statutes With Digital Guardian

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

Purpose-Built For Healthcare Systems

Full integration with 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 providers.

Allscripts
Centricity
Cerner
Epic
McKESSON Empowering Healthcare
MEDITECH Medical Information Technology, Inc.

A Trusted Partner

Many of the world's most renowned healthcare organizations rely on Digital Guardian to help secure their patient data.

Digital Guardian Is Deployed In More Than 120 Healthcare Systems

> **"Digital Guardian offers as an opportunity to not only better protect patient privacy, it gives us better insight into how our own sensitive data processes really work."**
>
> *VP IT Operations, Healthcare Insurance Provider*

> **"Our strategy is to educate employees and business associates through the policies we've set up. We use Digital Guardian to supervise and reinforce positive behaviors. We find people are much more careful with our sensitive data. Having this tool enables us to avoid being the 'IT Police'. We can give functionality back to our users knowing that information is being properly handled and protected."**
>
> *- Steve Scott, Information Security Manager, Saint Charles Health System*

St. Charles HEALTH SYSTEM

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.