FORTRA™

Meeting Stringent HIPAA Regulations

Your Guide To Safeguarding Patient Data

Table of Contents

Why Read This Guide?

In 2016, Security Professionals Were Faced With Two Critical Data Protection Issues:

1. The number of data breaches and cyberattacks increased throughout the year
2. HHS' Office for Civil Rights (OCR) continued to become more aggressive in enforcing HIPAA regulations

This eBook highlights important aspects of the Health Information Portability and Accountability Act (HIPAA) and describes how an appropriate Data Loss Prevention solution can help healthcare organizations effectively address both these issues.

OCR Continues Strict HIPAA Enforcements

Since March 2016 the OCR has been increasingly aggressive in bringing enforcement actions against healthcare organizations who have had PHI compromised through data breaches. The 2016 fines averaged $1.8M and aggressive enforcement is likely to continue now that OCR has resumed its HIPAA compliance audits. In just the first 19 days of 2017 the OCR had already published two HIPAA enforcement fines that totaled $2.7M.

$1.8M

Average OCR regulatory fine for HIPAA non-compliance in 2016

$23.5M

Total, OCR regulatory fines for HIPAA non-compliance in 2016

PART ONE

HIPAA 101

HIPAA Compliance Defined

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for securing sensitive patient data. Companies that deal with Protected Health Information (PHI) must have physical, network and process security measures in place and follow them to ensure HIPAA compliance. PHI includes any and all data that is collected by healthcare professionals which identifies an individual and determines appropriate care – such as demographic information, insurance information, medical history, tests and laboratory results.

Who Must Comply?

HIPAA compliance is mandated by the U.S. Department of Health and Human Services (HHS) for the following related healthcare organizations:

Covered Entities a “covered entity” is any organization or individual providing treatment, payment or operations in healthcare that directly handles PHI. This includes not just hospitals and doctors, but also health plan providers, healthcare clearinghouses, and any entity conducting certain financial and administrative transactions electronically such as electronic billing or fund transfers.

Business Associates a “business associate” is any organization or individual providing support in treatment, payment or operations that handles or discloses PHI. Whenever a covered entity contracts with a business associate to perform essential functions, they too are bound by the same standards under HIPAA.

Other Entities any healthcare contractor, subcontractor and other related business that has access to PHI must also maintain HIPAA compliance.

Compliance is More Important Than Ever

Healthcare providers and other entities dealing with PHI continue to migrate operations using technologies including computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy and laboratory systems. Similarly, health plans provide patient access to claims as well as care management and other self-service applications. As HHS rightly points out, while all of these electronic methods provide increased efficiency and mobility, they also drastically increase the security risks facing healthcare data.

HIPAA Is Comprised Of Four Core Regulatory Rules:

1. HIPAA Privacy Rule

2. HIPAA Security Rule

3. Breach Notification Rule

4. HIPAA Enforcement Rule

The HIPAA Security Rule and Privacy Rule both share the common goal of safeguarding patient PHI.

1. The HIPAA Privacy Rule

The HIPAA Privacy Rule established national standards for protecting certain individually identifiable health information. It requires appropriate safeguards to protect the privacy of PHI by setting limits and conditions on the uses and disclosures. The Privacy Rule also gives patient's rights regarding their health information, including the right to examine and obtain a copy of their health records as well as to request corrections.

The Privacy Rule requires healthcare organizations to consider the confidentiality, integrity and availability of PHI. Procedures need to be in place to address the use and disclosure of PHI and notice of privacy practices. It also prohibits the disclosure of patient genetic information under the Genetic Information Nondiscrimination Act (GINA). The Privacy Rule applies to all media types including paper, oral and electronic.

2. The HIPAA Security Rule

The HIPAA Security Rule established a set of national security standards for protecting specific health information that is held or transferred in electronic form. The Security Rule operationalizes the Privacy Rule's protections by addressing the technical and nontechnical safeguards that covered entities must put in place to secure individuals' electronic PHI (ePHI).

The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of ePHI. Within these requirements are 18 standards and 36 implementation specifications for organizations to address. Broadly drawn, covered entities should implement the following four ePHI protections:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information
3. Protect against reasonably anticipated, impermissible uses or disclosures
4. Ensure compliance by their workforce

The Security Rule is in place to protect the privacy of individuals' health information, while at the same time allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. It is flexible by design to allow a covered entity to implement policies, procedures and technologies that are suited to the entity's size, organizational structure and risks to patients' ePHI.

3. The HIPAA Breach Notification Rule

The Breach Notification Rule requires that breaches of unsecured PHI be reported to HHS. These regulations implemented section 13402 of the HITECH Act by requiring HIPAA covered entities and their business associates to comply. Similar breach notification provisions implemented and enforced by the Federal Trade Commission apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

4. The HIPAA Enforcement Rule

HIPAA compliance is mandated and enforced by the U.S. Department of HHS. Specifically its Office for Civil Rights (OCR) is responsible for enforcing the Privacy and Security Rules. The HIPAA Enforcement Rule contains specific provisions relating to compliance and investigations, the imposition of civil money penalties for violations, and procedures for hearings. According to the American Medical Association, penalties for noncompliance increase based on the level of negligence, with a maximum penalty of $1.5 million per violation. OCR publishes highlights of its monthly enforcement activities, enforcement data, case examples that resulted in corrective action, and resolution agreements.

What Is The HITECH Act?

HITECH

Health Information Technology for Economic & Clinical Health Act

In 2009 the U.S. government passed a supplemental law to help ensure HIPAA compliance: the Health Information Technology for Economic and Clinical Health (HITECH) Act. It was enacted to stimulate the widespread adoption of electronic health records (EHR) and supporting technologies while securely controlling the increased use, storage and transmission of this information. Simultaneously HITECH raised penalties on health organizations and their business associates that violate HIPAA Privacy and Security Rules. Finally the government provided financial incentives for the “meaningful use” of certified EHR technology in the Medicare and Medicaid programs.

PART TWO

Security Strategies For Protecting Patient Data

Security Components Of HIPAA Compliance

Physical Safeguards Include:

- Limited facility access and control with authorized access in place
- Policies defining use and access to workstations and electronic media
- Restrictions for transferring, removing, disposing and re-using electronic media or ePHI

Technical Safeguards Include:

- Access controls that allow only authorized personnel to access ePHI, including use of technologies such as unique user IDs, emergency access procedures, automatic log off, and encryption and decryption
- Audit reports or tracking logs that record activity on hardware and software
- Integrity controls, which are policy-based measures put in place to confirm that ePHI is not altered or destroyed
- IT disaster recovery and offsite backup to ensure that electronic media errors and failures are quickly remedied so that patient PHI is recovered accurately and intact
- Network security that ensures HIPAA compliant hosts protect against unauthorized access to ePHI by addressing all methods of data transmission including email, internet and private network such as a private cloud

Data Protection Strategy For HIPAA Compliance (And Beyond)

The need for data security has only grown with the proliferation of electronic patient data. Today's high-quality care requires healthcare organizations to meet this accelerated demand for data while protecting PHI/ePHI beyond the baseline requirements for HIPAA compliance. Many healthcare organizations are taking further steps to strengthen their data protection in the wake of costly data breaches that hit the industry in recent years.

A Data Protection Strategy For Hipaa Compliance (And Beyond) Should:

1. Ensure the security and availability of PHI to maintain the trust of practitioners and patients
2. Meet HIPAA and HITECH regulations for access, audit, and integrity controls as well as for data transmission and device security
3. Maintain greater visibility and control of sensitive data throughout the organization

Protecting patient privacy requires a combination of robust data security strategies as well as appropriate security solutions and sufficient IT resources to implement them. Security solutions commonly used in the healthcare industry include access control, data loss prevention, encryption, secure file sharing tools, and network security solutions such as firewalls and antivirus software.

PART THREE

DLP For HIPAA Compliance

DLP Protects Patient Data & Cuts Your Risk Of Fines

The best data protection solutions recognize and protect patient data in all its forms, including structured and unstructured data, emails, documents and scans. This allows healthcare providers to freely yet securely share data both inside and outside the organization to ensure the best possible patient care.

Data Loss Prevention (DLP) solutions are widely deployed in healthcare organizations because of their ability to discover, classify, monitor and protect ePHI. DLP is a powerful tool that provides a simple compliance framework to prevent the loss of PHI.

DLP Supports HIPAA Compliance In Three Primary Ways:

1. Analyzes potential risks to electronic PHI
2. Educates care providers on security policies - in real time
3. Periodically assesses security policies

1. Analyze Potential Risks To Electronic PHI

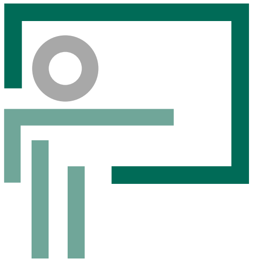
Protection starts with understanding the risks. The best DLP tools provide a number of mechanisms to analyze risks to PHI per the HIPAA Security Rule and limit PHI access to the "minimum necessary". Insist on the following key functions of any DLP solution:

- Discovers PHI stored on laptops, workstations, and servers that are unencrypted
- Measures PHI being emailed out of your organization
- Detects PHI being transferred out of your organization in unencrypted FTP
- Audits PHI being copied to USB devices or burned to CDs or DVDs
- Tracks and controls PHI in, or being uploaded to, the cloud

2. Educate Care Providers On Security Policies – In Real Time

Employees are any healthcare organization’s biggest risk. The best DLP tools prevent user actions that put the organization at risk and educate users in real time on the appropriate handling of PHI. Look for the following key functions in a DLP solution:

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



3. Periodically Assess Security Policies

What isn't measured can't be improved. The best DLP tools provide a mechanism to continuously assess security policies and procedures. Key DLP functions include:

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

PART FOUR

Digital Guardian Purpose Built For Healthcare

Why Healthcare Systems Choose Digital Guardian

Fortra™'s Digital Guardian® believes that data protection products for regulatory compliance are often needlessly complex to implement and difficult to manage, leading to unplanned costs, delays and diminished RoI. Digital Guardian for Compliance has taken a different approach.

DIGITAL GUARDIAN IS DEPLOYED IN MORE THAN 120 HEALTHCARE SYSTEMS

Free Download

Digital Guardian for Healthcare solutions sheet

Free Download

The Definitive Guide to DLP for Healthcare

HEALTHCARE CASE STUDY

PLUG THE LEAKS

SITUATION: St. Charles Health System (SCHS) of Oregon completed a security risk assessment that found PHI leaking via the Internet and unencrypted email.

SOLUTION: SCHS implemented Digital Guardian's compliance solution for ongoing data discovery, data monitoring and blocking. The solution provides DLP protection for all SCHS facilities across 3 hospitals, 20 clinics and nearly 3,000 caregivers. Preloaded with HIPAAcompliant policies, Digital Guardian began returning value immediately after being turned on. "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", said Steve Scott, InfoSec Manager. According to Scott, responding to alerts and refining policies, as management identifies new data to be registered, is all that's required from him and his team. He finds himself spending less then 30 minutes a day with the system.

RESULTS: SCHS can effectively enforce regulations while educating physicians, employees and partner providers about risky behaviors. "Our strategy is about changing employee and business associates' behavior through the policies we've set-up. We use Digital Guardian to supervise and reinforce the behavior," said Scott..

Read the Full Case Study

St. Charles Healthcare System

> **"Since implementing this DLP solution, we find people are much more careful with the organization's sensitive data. We can give functionality back to our users knowing that our data is being properly handled and protected."**
>
> **- STEVE SCOTT**
> **INFORMATION SECURITY MANAGER**
> **SCHS**

DLP On The Network, On Endpoints & In The Cloud

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

Our Cloud Data Protection allows healthcare organizations to adopt cloud storage while maintaining the visibility and control they need to comply with privacy and data security regulations.

Learn More

Digital Guardian for Compliance solutions

Enterprise DLP In 30 Minutes Or Less Per Day

Digital Guardian believes that products offered to address regulatory compliance are often needlessly complex in implementation and difficult to manage, leading to unplanned costs and delays. Digital Guardian has taken a different approach. Our technology for identifying and controlling compliance data such as ePHI is the industry’s most accurate. By focusing on protecting ePHI, Digital Guardian delivers a compliance solution that is recognized as the easiest to deploy and manage.

- Enhanced simplified management control for consistent uniform policy administration
- Powerful yet simple to deploy appliances designed for quick installation
- Easy modular growth by capacity, function and location

The Lowest False Positive Rate

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 triggered only 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**

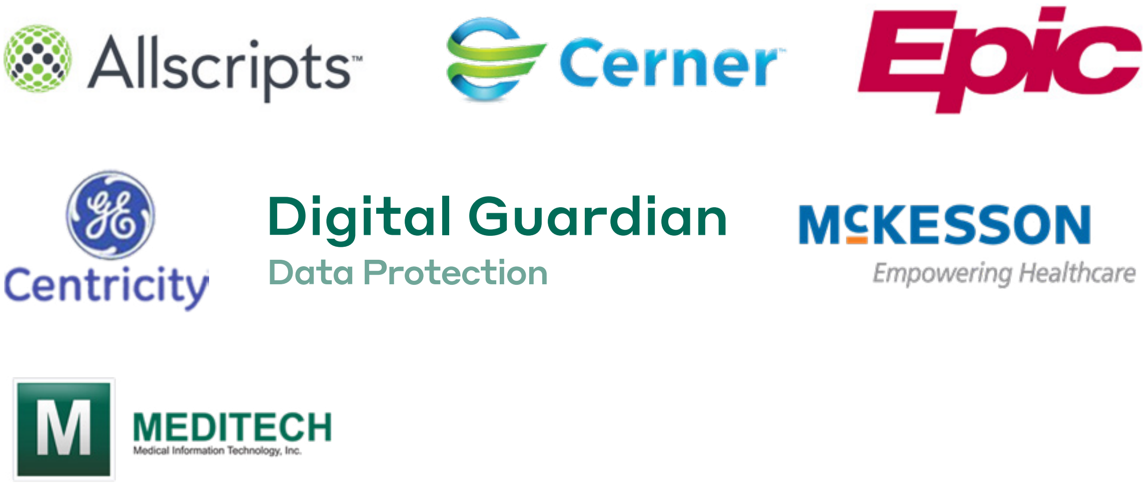
St. Charles HEALTH SYSTEM

Learn More

Digital Guardian Data Discovery

Fully Integrated With The Leading EHRs

Digital Guardian for healthcare is integrated and tested with the leading EHRs.



Our Experts Can Stop Ransomware Attacks Too

Cybercriminals have turned to ransomware as the latest go-to tool for attacking and extorting hospitals. With new ransomware variants introduced every day, traditional signature-based antivirus and threat detection methods are woefully ineffective.

Digital Guardian's Advanced Threat Protection Managed Security Program combines security researchers and analysts' expertise, Digital Guardian's Threat Aware Data Protection Platform and a centralized threat intelligence management system. This combination enables Digital Guardian to detect and remediate threats faster and more efficiently to provide you with the highest level of protection from ransomware.

DIGITALGUARDIAN
MANAGED SECURITY PROGRAM
FOR ADVANCED THREAT PROTECTION

FORTRA™

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.