HOWARD med TECHNOLOGY SOLUTIONS

SOPHOS
Security made simple.

Solution Brief

HIPAA/HITECH Compliance for Healthcare Organizations

Complying with the new HITECH Act data breach notification requirements

Introduction

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, includes the requirement to protect the privacy and security of individual's health information, defined as "protected health information" (PHI). The HIPAA regulation applies to "covered entities," which include healthcare providers (including hospitals, nursing homes, clinics, pharmacies, doctors, psychologists, dentists, chiropractors), health plans (including health insurance companies, HMOs, company health plans, Medicare, Medicaid, military/veteran healthcare programs) and healthcare clearinghouses (entities that process nonstandard health information they receive from another entity into a standard, such as standard electronic format or data content, or vice versa).

The HIPAA privacy and security regulations also extend to "business associates" (including third-party administrators, pharmacy benefit managers for health plans, claims processing/billing/transcription companies, persons performing legal, accounting and administrative work).

HIPAA/HITECH Compliance for Healthcare Organizations

The 2009 HITECH Act

The 2009 American Recovery and Reinvestment Act (ARRA), passed by the Obama administration, includes a section called the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act promotes adoption of "electronic health records" (EHRs) to improve efficiency and lower healthcare costs. Anticipating that the widespread adoption of electronic health records would increase privacy and security risks, the HITECH Act introduced new security and privacy related requirements for covered entities and their business associates under HIPAA, increased penalties for non-compliance, and extended enforcement authority to state attorneys general.

Data Breach Notification Requirements

The HITECH Act requires covered entities to notify affected individuals and the Secretary of the U.S. Department of Health and Human Services (HHS) in the event of a breach of "unsecured protected health information" (PHI), which the regulation defines as data that is not secured through the use of a technology or methodology to render it unusable, unreadable, or indecipherable to unauthorized individuals. The notification requirements vary according to the amount of data breached. A data breach affecting more than 500 people must be reported immediately to the HHS, major media outlets, and individuals affected by the breach. Also, the HHS secretary is required to post on an HHS website the list of covered entities that have reported breaches. A data breach affecting fewer than 500 people must be reported to the HHS secretary on an annual basis and to the individuals affected by the breach.

If a business associate is responsible for the data breach, then it must notify the covered entity, which is then expected to take the appropriate action.

The Cost for Non-Compliance

Fines for non-compliance with the HIPAA privacy rule have increased significantly under the HITECH Act. An organization can now be fined up to $1,500,000 per calendar year for each violation. An organization that has a data breach will incur monetary expenses associated with notifying people affected by a breach, customer loss, legal fees, fines, investigations and forensics, audits and consulting, and other costs that can quickly turn into a multimillion-dollar crisis. According to a 2010 study conducted by the Ponemon Institute, the average per-victim cost to a healthcare organization that suffered a data breach is $294.

In addition, individuals who have been impacted by a data breach can now receive a percentage of a civil law suit monetary settlement, which is an incentive for organizations that hold personal identifiable information (PII) to comply with HIPAA.

The risks, realities, and costs to healthcare organizations were illustrated when Connecticut's attorney general brought action against insurer Health Net under HITECH after a breach affecting 1.5 million customers, including more than 400,000 Connecticut residents. In addition to a $250,000 settlement, Health Net faces $375,000 in additional fines as well as pending lawsuits from other states.

Encryption and Control Provide a "Safe Harbor"

The HITECH Act also requires the issuance of technical guidance on the technologies and methodologies "that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals." The guidance specifies data destruction and encryption as actions that render PHI unusable if it fell in to the wrong hands.

HIPAA/HITECH Compliance for Healthcare Organizations

Challenges to Securing Protected Health Information

The endless network - The mobile health movement has redefined the endpoint. Implementation of EHRs driven by ARRA funding and the level of electronic interaction now required among covered entities, business associates and individuals have grown exponentially. Previously healthcare organizations needed to load anti-virus software on its users desktops, surround them with a firewall, and they were good to go. Organizations today are much more distributed and workers need access to data from anywhere and on just about any device – including iPads and smart devices. This means the previously defined notion of being "in" the network is no longer relevant and organizations are forced to ensure devices are protected no matter where they are to prevent risks to data integrity.

Sophos Provides Comprehensive Protection for Data at Rest, in Use and in Motion

Sophos solutions help enforce compliance with HIPAA by protecting the confidentiality of sensitive data (including PHI) and safeguard the reputation of your organization while allowing all legitimate users—patients, doctors, staff and business partners—to maximize their productivity, confident that their data is secure. Sophos solutions provide multi-layered security that includes encryption for PCs, portable media and email, device control, and data loss prevention. Sophos solutions protect data through its entire lifecycle (data at rest, in motion, in use and disposal) and at locations from the organization's core to the edge and beyond.

Sophos SafeGuard Enterprise protects data at the highest points of risk by providing full disk encryption for PCs and MACs (laptops, desktops), encryption of all types of removable media, and port control of physical and wireless ports on PCs for data leak prevention. The complementary technologies offered in the integrated solution are designed to greatly increase overall data security across the enterprise in the most cost-effective manner. The solution includes a single centralized management console. SafeGuard provides centralized security policy control, audit and log consolidation, key management and easy-to-use recovery tools to provide consistent data security for PCs and mobile devices in mixed device and OS environments.

Sophos Enduser Data Suite (EUDS) protects all your computers and data while leveraging your anti-virus budget. Simplified cross-platform security, centralized management, full disk encryption, data loss prevention and control of devices, applications and network access let you secure your business and comply with regulations. EUDS prevents the accidental loss of sensitive information with a unique and simple approach to content-aware data loss prevention (DLP) that integrates scanning into the anti-virus agent, reducing the need for a separate software installation. It protects transfers onto portable media, web uploads and email, and comes with access to the SophosLabs managed library of sensitive data definitions including a HIPPA category which provides detection of PHI, FDA approved drugs, and ICD-9 classified drugs.

Sophos Mobile Control lets you secure, monitor and control the configuration of smartphones and handhelds, including Apple iPhones and iPads, Google Android and Windows Mobile devices. Its web-based console centralizes management allowing over-the-air distribution of configuration settings, commands and applications and provides on-demand reports of compliance violations. Sophos Mobile Control prevents compliance

HIPAA/HITECH Compliance for Healthcare Organizations

violations by remotely wiping the lost or stolen devices with confidential data. It enables consistent security policy enforcement like requiring strong password to access the device and fine-grain control of all mobile devices irrespective of device type, operating system or carrier.

The HITECH Act's guidance on technologies clarifies "data in motion" to include "data that is moving through a network, including wireless transmission, whether by e-mail or structured data exchange..." To help healthcare organizations follow this guidance, Sophos also provides email encryption and end-to-end network file share encryption solutions to secure data in motion:

Sophos Enduser Data Suite
enables you to block malware and spam, and meet compliance requirements that mandate the encryption of sensitive data within email. Data protection is achieved using SPX email encryption and Sophos content-aware data loss prevention. Implementation is straightforward using preconfigured rules and a wizard driven policy manager. SPX ensures email is encrypted during transit and can be easily decrypted by the email recipient without the need to install additional software. The product also comes with access to the SophosLabs managed library of sensitive data definitions including a HIPPA category which provides detection of PHI, FDA approved drugs, and ICD-9 classified drugs.

SafeGuard Enterprise: For end-to-end network files, file share encryption automates file encryption and controls employee access to PHI files—stopping external threats and internal leaks. SafeGuard Enterprise ensures that PHI files remain encrypted on servers, across networks and when stored on end-user PCs until the moment authorized users choose to open the files. Flexible central management ensures end-user ease of use and transparency.

Contact your Sophos representative today to learn more about Sophos healthcare data protection solutions. Product demos and trial versions available on request.

HOWARD med TECHNOLOGY SOLUTIONS

General Information: 1 (888) 912-3151
Web: www.howard-medical.com

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

HIMSS Gold CORPORATE Member

SOPHOS