

Solution Brief

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 health information of individuals, 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).

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.

New data breach notification requirements

The HITECH Act requires covered entities to notify the 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”. The regulation defines unsecured protected health information (PHI) as PHI 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.

Penalties for non-compliance

The fines for non-compliance with the HIPAA privacy rule have increased significantly with the introduction of the HITECH Act. An organization can now be fined up to \$1,500,000 per calendar year for each violation.

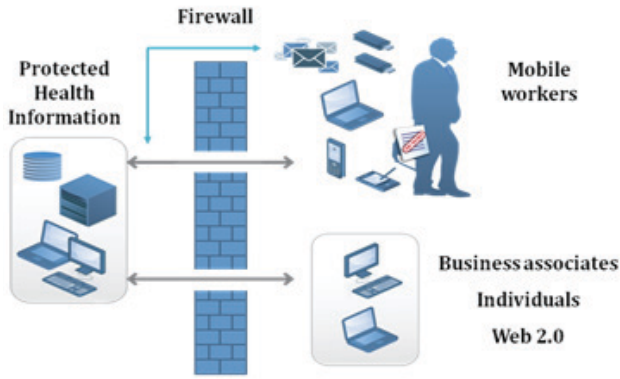
In addition, individuals who have been affected by a HIPAA data breach can now receive a percentage of a civil monetary penalty or monetary settlement. This financial provision may be enough of an incentive for organizations to comply with HIPAA.

In addition to fines, an organization that has a data breach will incur monetary expenses associated with notifying people affected by a breach. Once emails, first-class mailings, toll-free numbers, media outreach, work-hours and more are tabulated, a breach can quickly turn into a multimillion-dollar issue that could have been avoided.

Source: The above sections quote and paraphrase information from www.hhs.gov.

Challenges to securing protected health information

Digital generation set loose - There is now a greater degree of electronic interaction between covered entities, business associates and individuals, which is only expected to increase further as a result of the ARRA stimulus plan. At the same time, the old IT perimeter has dissolved. In the past, an organization simply could have loaded anti-virus software on its users' desktops and surrounded them with a firewall. But people work differently now and need access to all kinds of information, which has opened up organizational networks beyond the old perimeters. They use mobile devices, PDAs and memory sticks that can all leave the network, while organizations need to provide business associates and individuals with access to their networks. Web 2.0 has created all sorts of opportunities for data to be accessed by people who should not have access to it.



Encryption provides a “safe harbor” from data breach notification requirements

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. PHI that is encrypted and whose encryption keys are properly secured would provide a “safe harbor” to covered entities and would not require them to issue data breach notifications.

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 your sensitive data (including patient information) and safeguard the brand and 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, port and device control, and data leak 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 (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. It 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 Endpoint Security and Data Protection (ESDP)** protects all your computers and data without stretching your anti-virus budget. Simplified cross-platform security, centralized management, integrated data loss prevention, full disk encryption and control of devices, applications and network access let you simply secure your business and comply with regulations. It prevents the accidental loss of sensitive information with a unique and simple approach to data leak prevention (DLP) that integrates scanning into the anti-virus agent, reducing the need for a separate software installation. SophosLabs provides pre-defined DLP templates for common types of sensitive data.

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 to follow this guidance, Sophos also provides email encryption and end-to-end network file share encryption solutions to secure data in motion:

- » **Sophos Email Security and Data Protection:** Sophos integrates SPX encryption and advanced DLP capabilities into its line of Sophos Email Appliances to provide customers with a truly unique solution that offers affordable, simplified compliance. SPX encryption provides email encryption for sensitive information right to the recipient while making encryption deployment simple with its wizard-driven policy setup and tight integration with gateway email security. Sophos Email Security and Data Protection makes compliance simple and consistent across your entire organization, even for unmanaged endpoints, ensuring there are no unwanted leaks.
- » **SafeGuard LAN Crypt:** 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 LAN Crypt 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.