



IN-DEPTH SOLUTIONS BRIEF:

The HITECH Act:

Raising the Compliance Bar for HIPAA



The HITECH Act:

Raising the Compliance Bar for HIPAA



“Privacy is the key to implementing a successful health IT system Americans trust.”

—Coalition Letter to U.S. House Regarding HITECH Act, January 21, 2009

Key Definitions:

Breach

The unauthorized acquisition, access, use, or disclosure of protected health information that compromises the security or privacy of such information, except where the person to whom the information is disclosed would not reasonably have been able to retain such information or in certain specified circumstances of inadvertent disclosure or unintentional acquisition of the information.

Electronic Health Record (EHR)

An electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Personal Health Record (PHR)

Individually identifiable health information as defined under HIPAA that is contained in a personal health record and includes information that is provided by or on behalf of the individual and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Unsecured Protected Health Information (PHI)

Protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

Source: American Recovery and Reinvestment Act of 2009: Title XIII of Division A and Title IV of Division B (“HITECH Act”)

In 1996, the U.S. Congress passed the Healthcare Insurance Portability and Accountability Act (HIPAA), a comprehensive law designed to safeguard patient identities, medical records, health insurance activities and other protected health information (PHI). Thousands of hospitals, physicians, insurance providers, healthcare clearinghouses for nonstandard insurance claims, IT professionals, and other “covered entities” must meet HIPAA compliance requirements.

HIPAA compliance involves constant monitoring and regular assessments, especially for growing and evolving IT infrastructures. Encryption is usually part of a HIPAA-compliant security solution. As specified by the regulation, encryption means the “use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key,” and with such process or key not being breached. Audit trails for data access must also be generated and archived to provide critical information such as who accessed what, where, how and when.

Compliance is especially challenging where mobile devices are involved, which is very much the case in today’s healthcare industry. Medical professionals often use their own PCs, laptops and mobile devices to communicate across unsecured networks without encryption or other safeguards. Along with the possible theft or accidental loss of data from these devices, networks can be vulnerable to attacks and malicious activities by hackers, third-party service providers, technology vendors or healthcare employees.

The HITECH Act – New Teeth for HIPAA

Despite the challenges of compliance, the healthcare industry has made great strides in meeting its requirements, especially in terms of safeguarding PHI. However, critics have often charged that HIPAA enforcement by the U.S. Department of Health and Human Services (HHS) has been too lax. Other critics have charged that HIPAA security requirements should be strengthened and be applied to a wider range of entities.

¹ “Lock It or Lose It,” Harris Meyer, *Hospitals & Health Networks* magazine, September 2008.

² “Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research (2009),” Board on Health Sciences Policy (HSP).

The HITECH Act:

Raising the Compliance Bar for HIPAA



On February 17, 2009, President Obama signed into law a \$787 billion economic stimulus package called the American Recovery and Reinvestment Act (ARRA). Among many other things, the ARRA dedicates substantial resources to health information technology that supports the secure electronic exchange and use of health information. Title XIII of Division A and Title IV of Division B of the Act are referred to as the “Health Information Technology for Economic and Clinical Health Act” or “HITECH Act.” The HITECH Act includes a number of measures designed to broaden the scope and increase the rigor of HIPAA compliance. New updates to the law are added on a regular basis. In terms of the management and protection of PHI data, four key areas are especially important.

› **Extension of HIPAA rules to business associates**

The new law basically extends HIPAA privacy and security requirements to cover the business associates of covered entities. These business associates can include health information exchange organizations, regional health information organizations, or “any vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record.” Services can include legal support, accounting, IT, financial support, marketing and other areas. In effect, these associates are now subject to the same requirements for PHI data security as covered entities – along with the same penalties for noncompliance. The financial penalties for violations of HIPAA have also been increased, and a percentage of the civil penalties collected will be distributed to individuals harmed by the violations. The HITECH Act also provides that business associate agreements must be revised to include any new privacy or security requirements of the legislation.

› **Stricter requirements for breach notifications**

The HITECH Act requires that patients be notified of any unauthorized acquisition, access, use, or disclosure of their unsecured PHI that compromises the privacy or security of such information. Unless otherwise defined by the HHS, the HITECH Act defines unsecured PHI as any PHI that is not secured by a technology standard that renders it unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

IMPORTANT NOTE: For healthcare organizations, encrypted endpoint data on PCs or mobile devices is NOT subject to this breach notification requirement.

› **Encryption as a recognized methodology for protecting PHI**

The HITECH Act requires the secretary of HHS to issue guidance specifying the technologies and methodologies that render protected health information “unusable, unreadable or indecipherable” to unauthorized persons. This guidance was provided by the HHS on April 17th, 2009. Along with data destruction, encryption is cited as a compliant-appropriate methodology. In effect, the use of encryption can provide a “safe harbor” that protects covered entities and business associates from having to give notice under the breach notification provisions. HHS guidance identifies two encryption processes recognized by the National Institute of Standards and Technology (NIST) as rendering protected health information unusable, unreadable or indecipherable. For data at rest, the acceptable processes are those that are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. Valid encryption processes for data in motion (such as data moving through a network) are those in compliance with Federal Information Processing Standard (FIPS) 140-2.

The HITECH Act:

Raising the Compliance Bar for HIPAA



CREDANT SOLUTION

CREDANT Mobile Guardian (CMG) helps ensure that HIPAA and HITECH encryption and security requirements are consistently and efficiently enforced – regardless of where the data resides.

Only CMG enables organizations to:

- › Encrypt and secure data across multiple, diverse platforms from a single console.
- › Create automatic audit trails that offer proof of end-to-end data security.
- › Provide a transparent end-user interface that supports user productivity while keeping data safe.

CMG provides centrally-managed, highly scalable and architecturally flexible security to manage all data endpoints. With CREDANT, organizations can:

- › Provide endpoint data encryption to help avoid breach notification requirements.
- › Encrypt data using FIPS 140-2 compliant algorithms.
- › Provide all the necessary audit reports required by HIPAA and HITECH mandates.
- › Protect patient data from leaving the organization unprotected on USB flash drives or other forms of removable media.
- › Protect data from unwarranted access, thus reducing risk of internal breaches.

› Proactive enforcement

Organizations must move soon to gain maximum benefit from incentives – and to avoid penalties for non-compliance with the HITECH Act. Physicians can earn \$40,000 to \$60,000 over a five-year period if they implement health information technology according to regulations. For hospitals, payment incentives start at a rate of \$2 million annually. Additional amounts are provided based on the volume of Medicare-supported patients. The HITECH Act requires periodic audits to ensure that covered entities and business associates are in compliance with the requirements of the HITECH Act. If required technology is not in place by 2015, these incentives turn into penalties and payment cuts. Penalties for a single violation can total \$250,000, with a maximum of \$1.5 million for repeated or uncorrected violations.

Next Steps for Organizations

Every organization must address compliance requirements in terms of their unique business goals and technical environment. However, any compliance strategy under the HITECH Act should include the following initiatives:

- › Update Notice of Privacy Practices to reflect changes in privacy and security policies.
- › Update HIPAA privacy and security policies accordingly.
- › Determine whether an endpoint data protection including encryption enables the organization to avoid breach notification requirements of the HITECH Act and also any state law counterpart to the new federal breach notification provisions.
- › Expand business associate lists to include vendors and others.
- › Update Business Associate Agreements to include expanded new requirements.

Source: Based on USLaw.com http://www.uslaw.com/library/Health_Law/HITECH_Act_Signed_Law_High_Hope_Follows.php?item=383179