

“Getting Technical on the HITECH Act”

*Newly released by Scott G. Price, CPA, CISA, CIA
Director – A-lign CPAs*

Why was the Act needed?

Prior to the passage of the HITECH Act, organizations often did not report breaches of medical information that did not contain financial information. Under current HIPAA laws, notification of the breach is not required in certain circumstances. Consumer protection groups saw the void in the current law and wanted clear guidelines that must be followed in breaches of medical information that does contain financial information. Additionally, these groups sought to have significant penalties imposed on organizations that were not compliant with the new guidelines.

Understanding the Act

The Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of the American Recovery and Reinvestment Act of 2009 (ARRA) was issued on August 24, 2009 and took effect on September 23, 2009. The Department of Health and Human Services (HHS) acknowledged that it will take considerable effort for health plans to become compliant with the new requirements. To allow health plans to become compliant, HHS will not impose sanctions for failure to provide notice with respect to breaches discovered before February 17, 2010, however health plans are to make good faith efforts to comply immediately.

Currently, only covered entities, such as health care providers and health plans, are subject to the HIPAA privacy and security rules. Business associates, entities that perform a service or process on behalf of a covered entity which involves the use or disclosure of protected health information (PHI), were not previously subject to HIPAA. Rather, business associates only maintained liability that was on a contractual basis to the covered entity pursuant to the terms of the business associate agreement. That has changed under HITECH. The HIPAA privacy and security rules will now extend to apply to business associates as they apply to covered entities.

PHI is individually identifiable health information that is maintained or transmitted by a covered entity. The health information is “individually identifiable” if it is created or received by a covered entity, relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual, and identifies the individual, or there is a reasonable basis on the part of the disclosing entity to believe that the information may be used to identify an individual. HIPAA does not clearly define what “identifies the individual.” What it does state is that information which has been “de-identified” is not individually identifiable and therefore, is not PHI. De-identified information is where items such as name, address, dates of service, telephone number, Social Security number, and other unique identifiers are removed.

HITECH increases individuals’ rights under HIPAA. For example, individuals will now be able to deny health care providers from disclosing their PHI to a health plan for purposes of payment or health care operations if the individual pays for the health care item or service in full. In addition, individuals will now have the right to request and receive their PHI in electronic form if the covered entity maintains the information as an electronic health record (EHR). Further, covered entities maintaining PHI as an EHR have the obligation to supply requesting individuals an account of the uses and disclosures of those records for treatment, payment and health care operations purposes during the prior three years. Previously, individuals did not have the right to request an accounting of the uses and disclosures of their PHI for these routine purposes.

Impact of the Act

The HITECH regulations only require notification of a breach of unsecured PHI where the use or disclosure poses a “significant risk of financial, reputational or other harm to the individual.” Covered entities should perform and document a risk assessment to determine if harm has occurred and review factors such as to whom the information was disclosed, the type of information disclosed and what steps were taken upon discovery of the impermissible use or disclosure. For example, if the disclosed PHI simply identifies a patient and the fact he or she received benefits from a health plan, this may not constitute significant harm. However, if the disclosed PHI indicates the type of services the patient received (for example, mental health treatment) or if the disclosed PHI increases the risk of identity theft (such as a Social Security number) then there is a higher likelihood of harm.

The HITECH Act outlines specific notification requirements that must be followed by both covered entities and their business associates. In situations where more than 500 “residents of State or jurisdiction” have had their PHI breached, prominent media outlets serving that area must also be notified. Affected individuals should be notified and provided with basic information about the breach, including what corrective actions and investigation the covered entity is doing to prevent future breaches and mitigate losses. Reports to the Secretary of HHS describing any breaches are required to be made at least annually (where fewer than 500 breaches are reported) and immediately where more than 500 breaches of PHI are reported.

There are exceptions to the notification rules. First, any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if the acquisition, access or use was made in good faith and within the scope of the person’s duties and does not result in further use or disclosure in violation of the privacy rules. For example, a co-worker mistakenly sends an email with PHI to another co-worker who opens it in the normal course of business but then deletes it upon discovery and notifies the first employee. Secondly, an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another similarly situated person authorized to access PHI at the same covered entity or business associate and the information is not further used or disclosed in violation of the HIPAA privacy rule. For instance, a Human Resources employee who has authority to use or disclose PHI in order to administer the employer’s health plan is similarly situated to a finance employee who also has the right to use and disclose PHI in order to administer the employer’s health plan. In contrast, an operational employee who does not possess any responsibility regarding the health plan and has not been trained regarding the HIPAA privacy rules is not authorized to access PHI. Thirdly, a disclosure of PHI where a covered entity or business associate has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. For example, two persons with the same name (i.e. Bob Jones) work for the same employer. A Human Resources employee provides an enrollment form or explanation of benefits regarding the health plan to the wrong Bob Jones, recognizes the error and immediately takes back the document.

How can companies protect themselves from breaches?

One way to prevent personal information from being lost due to breaches is to never collect it in the first place. This method is the “minimum necessary” standard: only the information necessary to achieve clinical and/or research goals should be gathered. Defining and implementing this practice, particularly

with regards to disclosure of PHI, is left to the determination of covered entities and their business associates. Under the HITECH Act, the Secretary of HHS is directed to issue guidance on the “minimum necessary” standard, taking into account “the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease.

In reality companies must acquire and hold PHI. Therefore, they should do the following:

- Secure PHI through encryption of destruction
- Evaluate existing privacy and security policies and procedures and assess whether current administrative, technical and physical safeguards are adequate to protect the privacy and security of PHI.
- Draft and Adopt Incident Response plan with breach notification policy.
- Establish procedures and indentify an incident response team to respond to breach.
- Identify business associates that have access to PHI
- Consider incident response insurance policies.

In addition, covered entities should amend their agreements with business associates and require the business associates to assist in satisfying this compliance requirement.

Scott G. Price, CPA, CISA, CIA

Director – A-lign CPAs

About the Author

Scott Price is a director at A-lign with over 10 years of experience providing risk advisory services including SAS 70 and internal audits, business process reviews, and regulatory compliance assessments. Scott is a Certified Public Accountant, Certified Information Systems Auditor and Certified Internal Auditor.