



HITECH Issues Final Regulations on Protected Health Information Under HIPAA

Have you watched a movie and noticed the plot shift giving you the feeling that something big was about to happen? This shift in plot often causes a variety of emotions as the storyline begins to play itself out.

A similar thing is beginning to play itself out in the healthcare world through recent legislation known as the HITECH Act (The Health Information Technology for Economic and Clinical Health Act) that was enacted on February 17, 2009 and became effective September 23rd, 2009. HITECH is part of the American Recovery and Reinvestment Act of 2009 (ARRA) and impacts individuals, health-care providers, hospitals, health care plan sponsors, and their business associates such. Since the legislation was signed by President Obama, it's been a source of anxiety with many plot twists and turns.

ARRA addresses a number of things but in the healthcare space it provides funding for health information technology to facilitate adoption of electronic health records (EHR) by healthcare providers. HITECH requires covered entities under HIPAA (Health Insurance Portability and Accountability Act of 1996) and their business associates to provide notification in the case of a breach of unsecured protected health information (PHI).

Understanding HITECH is time consuming but necessary as unlike HIPAA, it has big teeth. Covered entities will be subject to large penalties beginning February 18, 2010 for any breach of unsecured protected health information. Business associates will be subject to penalties beginning February 17th, 2010. The HITECH act impacts individual's rights, covered entities, and business associate agreements in terms of breach notification which applies to electronic and paper records, the accounting for disclosure of PHI, the use of encryption, and the increase in enforcement and penalties for a breach of privacy or security requirements. Penalties can range from \$25,000 to \$1.5 million and will apply even if a

person did not know (and by exercising reasonable due diligence would not have known).

One confusion aspect of this legislation is the role of The Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC). HIPAA covered entities must notify HHS of any breach in unsecured PHI while non-covered entities under HIPAA must report a breach of unsecured PHI to the FTC.

To understand the basics of HITECH, it may be helpful to define a few terms such as PHI, unsecured PHI, and breach. HHS defines them as:

“PHI” - *protected health information” is the individually identifiable health information held or transmitted in any form or medium by these HIPAA covered entities and business associates, subject to certain limited exceptions.*

“Unsecured PHI - *unsecured protected health information” is “protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance” and provides that the guidance specify the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.*

“Breach” - *breach is the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information. The Act provides exceptions to this definition to encompass disclosures where the recipient of the information would not reasonably have been able to retain the information, certain*

¹ <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>

Continued from Page 1

unintentional acquisition, access, or use of information by employees or persons acting under the authority of a covered entity or business associate, as well as certain inadvertent disclosures among persons similarly authorized to access protected health information at a business associate or covered entity.

To aid covered entities in compliance, HHS provides a safe harbor rule where “covered entities and business associates that implement the specified technologies and methodologies with respect to protected health information are not required to provide notifications in the event of a breach of such information that is, the information is not considered “unsecured” in such cases.” Encryption and destruction are the two specified technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

Covered entities must now consider implementing encryption to safeguard electronic protected health information even if it decides not to encrypt it in favor of another method. Encryption provides a safeguard method to meet the new breach notification requirements while choosing other methods require covered entities to provide breach notification.

Through encryption or destruction PHI is considered to be secure from breach vulnerability and rendered unusable, unreadable, or indecipherable to unauthorized individuals if these processes are consistent with appropriate National Institute of Standards and Technology (NIST) publications for data in motion, data at rest, data in use, or data disposed.

Regarding potential breach violations, covered entities should consider whether an incident involved protected health information as much of the health information may not be PHI. For example, the health information would need to be individually identifiable such as but not limited to Social Security numbers, dates of birth, or email addresses. Consideration should also be given to whether the HIPAA Privacy Rule has been violated as it establishes the basis for the permitted use and disclosure of PHI. Also, when considering possible violations of the Privacy Risk Rule, note that notification is not required unless the violation poses a significant risk of financial, reputational, or other harm to the individual.

Breach notification varies depending on the affected individual (s). For example, notification for an unemancipated minor should go to the minor’s parents. For deceased individuals, notification goes to the next of kin or personal representative. If the breach involves 500 or more individuals, notification must go to HHS and the affected individuals and in some circumstances may require notification to the media serving the state or jurisdiction.

HITECH amends HIPAA’s Privacy Rule with various administrative requirements applying to breach notification. For example, covered entities and business associates must develop written policies and procedures, train workforce members and have sanctions for workers that fail to comply. In addition, there is a burden to demonstrate that all notifications were made as required.

This information is not intended as legal advice. Please rely on your attorney for professional guidance on the breach notification requirements.

² Available at <http://www.csrc.nist.gov/>

For more information, contact us at:

8000 GSRI
Building 3000
Suite 106
Baton Rouge, LA 70820
225.709.0334



MANAGE-TRAK
www.manage-trak.com