The HITECH Act: Congress Includes Sweeping Expansion Of HIPAA And Data Breach Notification Requirements In Stimulus Bill

 Derived from an article by James B. Wieland, Ober|Kaler

The American Recovery and Reinvestment Act of 2009, the “Stimulus Bill,” includes Title XIII—“Health Information Technology,” also known as the “Health Information Technology for Economic and Clinical Health Act” or “HITECH Act.” The HITECH Act contains significant expansions of the HIPAA Privacy and Security Rules and numerous other changes that will have a major impact on the healthcare information and technology sector. Virtually every healthcare provider and third-party service provider that stores or accesses individuals’ medical information will be affected by this new federal law.

In general, the effective date of the Improved Privacy and Security Provisions appears to be 12 months after February 17, 2009. However, there are a number of provisions with different effective dates and additional guidance from Health and Human Services is expected.

Following is a summarized list of the new requirements. All of Purdue’s covered components will be affected in some way.

- The HIPAA security requirements for administrative, physical, and technical information safeguards and written policies and procedures will apply directly to Business Associates as well as civil and criminal penalties for violations.
- Federal law now requires consumer notification of data breaches involving “unsecured” PHI. Both Covered Entities and Business Associates must comply.
- Vendors of personal health records and their service providers made subject to the same security breach notification requirement.
- Individuals may require Covered Entities not to disclose certain self pay services to health plans.
- The limited data set becomes a default minimum necessary standard.
- Covered Entities using electronic health records (EHRs) are required to provide accounting of disclosures of PHI for treatment, payment, and healthcare operations.
- Health Information Exchanges are brought specifically within Business Associate requirements.
- Restrictions on the remuneration for “sale” of EHRs or PHI
- Covered Entities with EHRs must provide an individual’s information in electronic form and transmit it to third parties, on the individual’s request.
- The HIPAA healthcare operations exception for “marketing” communications is narrowed significantly, if direct or indirect remuneration is received.
- Individuals must be given a right to opt-out of receipt of Covered Entity’s fund raising communications.
- The Act provides for “Improved Enforcement”. This includes periodic audits by Health and Human Services and the ability for individuals who have been harmed by an act of noncompliance with HIPAA, to receive a percentage of any civil monetary penalty or monetary settlement collected with respect to the offense.

Implementation plans are currently under development and detailed information will be provided to the HIPAA Steering and HIPAA Liaison Committees beginning in April 2009.

Where can I find the latest forms and other information about HIPAA?

The HIPAA Privacy Compliance Office has developed a website for Purdue staff to access forms and other HIPAA-related information. To access the site, please visit: http://www.purdue.edu/hipaa or contact: Joan Vaughan, Director, HIPAA Privacy Compliance telephone: (765) 496-1927 e-mail: jvaughan@purdue.edu
How to Tell, What to Do, If Computer is Infected?

Written by Cindy Welch, ITNS
Computer-virus infections don’t cause your machine to crash anymore. Criminals behind today’s infections usually want your computer operating in top form so you don’t know something’s wrong. That way, they can log your keystrokes and steal any passwords or credit-card numbers you enter at Web sites, or they can link your infected computer with others to send out spam.

Here are some signs your computer is infected, tapped to serve as part of “botnet” armies run by criminals:

You experience new, prolonged slowdowns. This can be a sign that a malicious program is running in the background.

You continually get pop-up ads that you can’t make go away. This is a sure sign you have “adware,” and possibly more, on your machine.

You’re being directed to sites you didn’t intend to visit, or your search results are coming back funky. This is another sign that hackers have gotten to your machine.

So what should you do?

Having anti-virus software here is hugely helpful. For one, it can identify known malicious programs and disable them. If the virus that has infected your machine isn’t detected, many anti-virus vendors offer a service in which they can remotely take over your computer and delete the malware for a fee. Purdue University affiliates can visit https://www.purdue.edu/securespurdue/download to download the latest version of the McAfee VirusScan software for your operating system for FREE. For a Windows system on your personally-owned equipment, this is VirusScan Home Edition Version 12.

You may have to reinstall your operating system if your computer is still experiencing problems. It’s a good idea even if you believe you’ve cleaned up the mess because malware can still be hidden on your machine. You will need to back up your files before you do this.

How do I know what information has been taken?

It’s very hard to tell what’s been taken. Not every infection steals your data. Some just serve unwanted ads. Others poison your search result or steer you to Web sites you don’t want to see. Others log your every keystroke. The anti-virus vendors have extensive databases about what the known infections do and don’t. If you are using our free McAfee Software as mentioned above, you can visit McAfee Threat Center at http://www.mcafee.com/us/threat_center/default.asp. Comparing the results from your virus scans to those entries will give you a good idea about what criminals may have snatched up.

For more information about computer security at Purdue, please access: http://www.purdue.edu/securespurdue/

FAQ of the Month...Continued

Avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information. In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use. Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.

Further, covered entities must ensure that their workforce members receive training on and follow the disposal policies and procedures of the covered entity, as necessary and appropriate for each workforce member. Therefore, any workforce member involved in disposing of PHI, or who supervises others who dispose of PHI, must receive training on disposal. This includes any volunteers.

Thus, covered entities are not permitted to simply abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons. However, the Privacy and Security Rules do not require a particular disposal method. Covered entities must review their own circumstances to determine what steps are reasonable to safeguard PHI through disposal, and develop and implement policies and procedures to carry out those steps. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the form, type, and amount of PHI to be disposed. For instance, the disposal of certain types of PHI such as name, social security number, driver’s license number, debit or credit card number, diagnosis, treatment information, or other sensitive information may warrant more care due to the risk that inappropriate access to this information may result in identity theft, employment or other discrimination, or harm to an individual’s reputation.

In general, examples of proper disposal methods may include, but are not limited to:

For PHI in paper records, shredding, burning, pulverizing, or other similar means of destroying the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.

For PHI on electronic media, clearing (using software to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

Other methods of disposal also may be appropriate, depending on the circumstances. Covered entities are encouraged to consider the steps that other prudent health care and health information professionals are taking to protect patient privacy in connection with record disposal.

FAQ of the Month...Continued

Derived from guidance provided by the Office for Civil Rights

Question:
What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information?

Answer:
The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), in any form. This means that covered entities must implement reasonable safeguards to limit incidental, and