HITECH Sticks

PATIENT'S PRIVACY IS HIGH PRIORITY

By Lynne Kottman, CHBME, CCP

The American Recovery and Reinvestment Act of 2009 (ARRA) found in Title XIII, created the Health Information Technology for Economic and Clinical Health Act or the HITECH Act. Much of the discussion of the HITECH Act in the medical community focuses on the carrot of potential payments to providers for adopting electronic medical records. As billing agents for medical providers, we need to also direct our attention to some of the stick portions of HITECH, specifically the Security Requirements and the Breach reporting requirements, which is the focus of this article. While most requirements of HITECH went into effect on February 17, 2010, Breach Reporting requirements went into effect on September 23, 2009.

Breaches are defined as the unauthorized acquisition, access, use, or disclosure of unsecured Health Information - via electronic, paper or verbal means which compromises the privacy/security of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. As you can see from this definition, information security that once only applied to electronic patient health information (PHI) now includes paper and verbal versions of patient information.

Unsecured is defined as "not protected by technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individual using technology specified by the Health and Human Services (HHS) Secretary." The standard set for appropriate encryption of data in motion is Federal Information Processing Standard (FIPS) 140-2. For data at rest, the encryption must be consistent with National Institute of Standards and Technology (NIST), Special Publication 800-111. The government considers information to be secured when it is encrypted, using the proper governmental protocols, or effectively destroyed. Destruction for paper records means at a minimum destroying them with a cross-cut paper shredder. If all of your information is encrypted to government standards when in motion, at rest, or in storage, you have earned a free pass on reporting breaches.

Some examples of a breach might include:

- PHI is disclosed pursuant to an attorney subpoena without obtaining necessary authorizations;
- Incorrect guarantor information is transmitted from a facility and a statement is subsequently sent to an incorrect address; and
- Unencrypted PHI is sent over the internet, intercepted, and used for illegal purposes.

> If all of your information is encrypted to government standards when in motion, at rest, or in storage, you have earned a free pass on reporting breaches.

It is important from a compliance perspective that you establish a policy for how to handle breaches when they occur. The following is an example of a Breach Policy:

> Company will identify, mitigate, investigate, evaluate and, when determined appropriate, report breaches of protected health information to the affected individual(s) and to the Secretary of Health and Human Services (HHS) following the requirements of HHS rules and regulations as outlined in the Federal Register/Vol. 74, No.162.

Some of the common ways breaches are identified include:

- Providers or business associates being contacted by an outside source, or contacted by a patient, or related party, or identification by an employee; and
- Problems become apparent with system transmissions or mail or attempts at intrusion in the computer system.

To date the largest volume of breaches have occurred from lost or stolen laptops or other electronic devices. When potential breaches are identified one of the essential first steps includes attempting to mitigate the breach. It is important to immediately stop any processes that would allow breaches to continue. Mitigation can include making attempts to retrieve information prior to disclosure and if not retrieved to request information be appropriately destroyed or returned. It is also important to identify when information would not have reasonably been retained.

Once a breach has been identified, mitigated, and investigated, it is important to determine if the breach has to be reported. First, the breach must be reported to the covered entity since the covered entity is required to report every breach to the Secretary of HHS. The covered entity can assign some of these responsibilities to a Business Associate in a Business Associate Agreement.

The following are allowable exceptions to the reporting requirements:

- Unauthorized persons to whom such information if disclosed, would not reasonably have been able to retain such information;
- Unintentional access or use by an employee of a covered entity (CE) or a business associate (BA);
- Inadvertent disclosure within a facility operated by a CE or BA;
- Encrypted electronic PHI; and
- Inadvertent disclosure to any other entity covered by a BA agreement, such as an insurance company.

The Breach Risk Assessment Process requires asking a number of pertinent questions to help determine if the breach reaches the level of "posses a significant risk of financial, reputational or other harm to the individual." An example of a simple work sheet that can be used to follow the required steps in determining if a breach is reportable can be found on page 27. It is important that any analysis be documented and kept on file to document the process followed in making any determination.

When a reportable breach occurs it is required that the covered entity (or agent, if responsibility was assigned in a B.A.) notify the individual, or next of kin if deceased, and do this in writing by U.S. first-class mail or by email (with prior patient agreement) without any delay. Notice must be provided within 60 days of discovery of the breach. Discovery is established when the party knew, was *(continued on next page)*

(*HITECH Sticks* continued)

notified or should have known.

- A notice must contain all of the following elements:
- Brief description of what happened/occurred;
- Information that was disclosed;
- Protective steps the patient/individual must now take him/herself;
- Actions being taken to investigate and mitigate the problem, as well as prevent any future recurrence of the same thing happening; and
- Contact procedures like a toll-free telephone number, email address website, or postal address.

Breaches that involve fewer than 500 individuals in any given state require that the covered entity keep a log of all reported breaches and log on and report at the year's end using the reporting form on the DHHS website.

Breaches involving 500 plus individuals must be reported immediately to the Secretary of DHHS and reported to individuals in accordance with the instructions provided on the DHHS website.

For breaches involving more than 500 residents in a single state in addition to reporting to the patient, and the Secretary, the breach must be reported to prominent media outlets.

If less than 10 notices do not have a good address, they can be conveyed via phone contact or email. If more than 10 have no good address, information must be posted prominently on the home page of the covered entity's website and must remain there for 60 days.

HITECH now obligates business associates to comply with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA) Security Rule's administrative, physical and technical safeguards and business associates are required to notify covered entities of breaches of unsecured PHI. In addition, civil and criminal penalties for violations now apply directly to business associates. These penalties have been significantly increased and are as follows:

Violations and Penalties

Tier I

If the organization in violation couldn't reasonably have known then the penalty will typically be $100 to $25,000 maximum fine per year.

Tier II

If the organization in violation had reasonable cause but not willful neglect then the penalty will typically be $1000 to $100,000 maximum fine per year.

Tier III

If the organization in violation is guilty of willful neglect but corrects the violation within 30 days, then the penalty will typically be $10,000 to $250,000 maximum fine per year.

Tier IV

If the organization in violation is guilty of willful neglect and does not correct the violation within 30 days, then the penalty will typically be $50,000 to $1.5 million. There is no maximum fine per year in this case. Criminal action is possible.

States' Attorney Generals can now bring suits under HITECH. HITECH also establishes an almost qui-tam-like methodology in that while there is still no private right of action under HITECH, a person harmed by a disclosure of health information may recover a portion of civil monetary penalties. Once this information is publicized, it could stimulate increased breach reporting by patients. HITECH also clarifies that criminal penalties apply to individuals in violation if the violation was willful and knowing.

Another provision of the HITECH that is highly problematic to both covered entities and their billers is the requirement that if a patient has paid the bill out of pocket, they can request that information not be shared with their insurance company. Unlike previous requests under HIPAA, the provider can no longer select whether to honor these requests. This could also pose additional problems if, for example, this request was made by a Medicare patient, where the government requires the provider files a claim on behalf of the patient. There are also multiple areas where communication problems could occur that make this a dangerous proposition for billers.

With the increased responsibility involved in maintaining the privacy and security of PHI, and the potential penalties that come from breaches, companies will be required to improve their HIPAA/HITECH policies and procedures and heighten vigilance to avoid creating breaches. Consequences of breaches that require reporting could impact client trust, cost large sums of money, and incur loss of client business. Additional information about the breach reporting can be located in the Federal Register/Vol. 74, No.162. For additional information go the to the OCR website www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html ■

Lynne Kottman, CHBME, CCP is the Corporate Compliance Officer of PracticeMax/MedaPhase. She serves on the HBMA Ethics and Compliance Committee and is also a member of the Council of Ethical Organizations' Health Ethics Trust. She can be reached at lynnekottman@practicemax.com.

Breach Notification Worksheet

Name of Patient		
Date of Breach **Date of Identification**		
Date of Evaluation **Determination-**	**Reportable**	**Non-Reportable**

PHI - Breach – Risk Assessment

1. To whom was the information impermissibly disclosed?

2. What immediate steps were taken to mitigate the potential harm to be less than "significant?"

3. Was PHI retuned prior to being accessed for an improper purpose?

4. The type and amount of PHI involved in the disclosure.

Report Necessity Determination

Did the incident pose a "significant risk for financial, reputational, or other harm to the individual?"

Assessor
Date of Report (if Reportable) **Date of Determination**
Reported to

Billing Entity Name **Compliance Department**