physician connection 2011
PROFESSIONAL SOLUTIONS INSURANCE COMPANY BRINGS YOU PRACTICAL TIPS FOR AVOIDING A MALPRACTICE ALLEGATION
Bonus Article

Handling Breaches of Protected Health Information (PHI)

Dr. Simpson was getting ready to close up for the day when his practice administrator, Bruce Johnson, came into his office, closing the door behind him. "You'd better sit down for this," Bruce said.

Bruce then proceeded to break the bad news. "After I met with our PPO reps about our billing issues, I ran a few other errands before heading back to the office. When I got back to my car, my laptop—downloaded with over 600 patient files, complete with medical information and billing information—was gone!"

If this happened to you, what would you do? Would you know how to comply with the new Health Information Technology for Economic and Clinical Health (HITECH) Act requirements for breaches in PHI?

Increased Monetary Penalties

HITECH is a specific part of the American Recovery and Reinvestment Act of 2009[1] intended to stimulate use of electronic health records (EHRs) by healthcare facilities and providers. In addition to promoting the adoption of EHRs, the Act also calls for strengthened enforcement and harsher penalties for privacy and security violations.

Prior to HITECH, civil monetary penalties for violating HIPAA were capped at $100 per violation and a maximum of $25,000 for identical violations in a calendar year. HITECH increases the penalties to range from $100 to $50,000 per violation and up to $1,500,000 per year. The new civil monetary penalties apply to violations occurring on or after February 18, 2009.

Another significant change is that a covered entity or business associate will now be subject to civil monetary penalties ranging from $100 to $50,000 ***even if they did not know of the violation.*** Prior to HITECH, lack of knowledge about a violation was an allowable defense. There are now four specific categories of violations and associated penalties:

Violation Category	Civil Monetary Penalty *per Violation*	Cap for All Identical Violations per Calendar Year
The covered entity did not know of the violation.	$100-$50,000	$1,500,000
The violation was due to reasonable cause and not willful neglect.	$1,000–$50,000	$1,500,000
The violation was due to willful neglect, but was corrected within 30 days of discovery.	$10,000–$50,000	$1,500,000
The violation was due to willful neglect, but was not corrected within 30 days of discovery.	$50,000	$1,500,000

[1] Pub. L. No. 111-5 (Feb. 17, 2009).

Specific penalties will be based on the nature and extent of the violation, the nature and extent of the resulting harm, and other factors. These may include prior compliance with the rules or the financial condition of the covered entity or business associate at the time of the violation. Obviously, these changes convey the message that PHI breaches will not be taken lightly.

Notification Requirements

HITECH also expands notification requirements when PHI has been breached. Effective February 22, 2010,[2] any healthcare facility or provider defined as a covered entity under HIPAA must provide notification of the breach to the affected individuals, the Secretary of the Department of Health and Human Services (HHS), and, in certain circumstances, to the media.

The notification rule applies when there is "acquisition, access, use or disclosure" of unsecured PHI in a manner that violates the HIPAA Privacy Rule and poses a "significant risk of financial, reputational or other harm to the individual."

However, notification is *not* required if:

- The breach was made in good faith by, and within the scope of duty of someone under the authority of a covered entity or business associate, and no further use or disclosure prohibited by the Privacy Rule occurs.
- There is an inadvertent disclosure by one person at a covered entity or business associate who is authorized to access PHI to another person at the same covered entity or business associate who is also authorized to access PHI, and no further use or disclosure prohibited by the Privacy Rule occurs.
- There is a disclosure of PHI and the relevant covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.
- The unsecured PHI has been rendered unusable, unreadable or indecipherable to unauthorized individuals.

NOTE: If a law enforcement agency determines notification would impede a criminal investigation or cause damage to national security, notification may be delayed. The delay can be for up to 30 days as *orally* directed by the law enforcement agency, or for longer if instructed *in writing.*

In consultation with legal counsel, a practice should review and analyze each *possible* breach of PHI to determine if it meets the definition and if a HIPAA violation has occurred.

After a Breach

If a breach has occurred, the following notification requirements apply:

Individual Notice: A practice must notify affected individuals following the discovery of a breach of unsecured, protected health information. This individual notice must be provided in writing via first-class mail or by e-mail if the affected individual has agreed to electronic notices.

If the practice has insufficient or out-of-date contact information for 10 or more individuals with breached PHI, it must provide a substitute individual notice. This can be done by posting a notice on the practice's website home page or by notifying major print or broadcast media in areas where the affected individuals are likely to reside.

If the practice has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide an alternative form of written, telephone or other means. The practice must provide these individual notifications without unreasonable delay and no later than 60 days after discovering the breach. The notification must include, to the extent possible, the following information. (See Sample Breach Notification Letter.)

- A description of the breach.
- A description of the types of information involved in the breach.
- The steps affected individuals should take to protect themselves from potential harm.

[2] 45 CFR 164.408.

- A brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches.
- Contact information for the covered entity.
- A toll-free number for individuals to call to determine if their protected health information was involved (if notices were provided via the web or major media).

Media Notice: If a breach affects more than 500 residents of a state or jurisdiction, the practice or other covered entity must notify prominent area media outlets in addition to the affected individuals. This notification may be provided in the form of a press release to media outlets serving the affected area.

Like individual notices, the media notification must be provided without unreasonable delay and no later than 60 days of discovering a breach. It must include the same information as the individual notice.

Notice to the Secretary: In addition to notifying affected individuals and the media as appropriate, covered entities must notify the HHS Secretary of breaches by visiting http://transparency.cit.nih.gov/breach/index.cfm and electronically submitting a breach report form.

If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and no later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches annually. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred. (See Sample Breach of PHI Log.)

Notification by a Business Associate: Before HITECH, business associates' obligations were limited to their contractual obligations with the covered entities. Under HITECH, however, business associates are statutorily subject to all HIPAA security provisions, including physical and technical PHI safeguards, the development of security policies and procedures, and staff training programs on PHI protection.

If a breach of unsecured PHI occurs by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should identify each individual affected by the breach and provide to the covered entity any other information required to notify affected individuals.

Violations by business associates will result in the same civil and criminal penalties as a covered entity. [Note: Enforcement of the Business Associates Liability provision has been delayed until a final rule has been issued.]

Public Posting of PHI Breaches: Under HITECH, the Secretary of HHS is required to publicly post a list of breaches of unsecured protected health information affecting 500 or more individuals. This list can be found at: www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

As of December 2010, the list contained over 200 breaches, with brief case summaries of the cases investigated and closed, as well as the names of providers who have reported breaches of unsecured protected health information to the Secretary. Approximately 30 percent of these breaches involved PHI stored on laptops, followed by breaches occurring with paper records, and then breaches on desktop computers and personal electronic devices.

What Can We Learn?

In the scenario at the beginning of this article, more than 500 patients were involved. Consequently, Dr. Simpson and his practice would be required to do the following within 60 days of discovering the breach:

- Send a letter to each of the 600+ patients about the breach. This letter should be sent earlier than the 60-day requirement, if possible, to mitigate damages for both patients and the practice.
- Notify the local media with an objectively stated description of what occurred.

- Report the breach to the HHS Secretary using the online reporting form.

Practices are encouraged to maintain a log of all PHI breaches throughout the year for ease of reporting. This task can be assigned to the practice administrator or a designated privacy officer.

Existing policies and procedures dealing with PHI should be reviewed by the practice, with input from physicians, practice administrators, IT staff or security consultants, and legal counsel to ensure compliance. It's also important to initiate a well-thought-out breach incident response plan to promptly identify and report any possible PHI breach. [Note: State law may preempt HITECH if it is more proactive. Legal counsel should be consulted if there are questions about which applies.]

Breach of PHI can have serious financial ramifications for the practice and its patients. Additionally, the notification requirements are very time-sensitive and delays can result in hefty monetary penalties for the practice. However, prompt breach discovery and notification can mitigate those consequences. That's why routine HIPAA education programs should stress the importance of clear reporting that avoid delays.

Professional SOLUTIONS | INSURANCE COMPANY

Send all inquiries, address changes and correspondence to:
Physician Connection, P.O. Box 9118, Des Moines, IA 50306

Toll-Free 1-800-718-1007, ext. 9187
Internet – www.psicinsurance.com
Email – submissions@psicinsurance.com

Physician Connection is published for policyholders of Professional Solutions Insurance Company. Articles may not be reprinted, in part of in whole, without the prior, express consent of Professional Solutions.