Under HITECH, What are Your Client's Obligations When There is a Breach of Patient Records?

Michael F. Schaff, Esquire
Glenn P. Prives, Esquire
Wilentz Goldman & Spitzer PA
Woodbridge, NJ

Introduction

Many medical practices are not aware that the failure to notify patients of the breach of their unsecured Protected Health Information (PHI) may result in the U.S. Department of Health and Human Services (HHS) sanctioning this practice. When such a breach has been discovered by the practice, it is mandatory for the practice to provide notice of the breach to the affected patients and to the HHS Secretary, in accordance with recent legislation. In 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH Act) as part of the American Recovery and Reinvestment Act of 2009. The HITECH Act established new federal breach reporting requirements for medical practices when the PHI of the practice's patients is compromised.[1] Some of the more ambiguous HITECH Act provisions were clarified by subsequent regulations that HHS promulgated on August 24, 2009.[2]

Pursuant to these regulations, the HITECH Act defines a "breach" as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."[3] The statutory definition of a breach does not include an unintentional, one-time acquisition or use of this information by an individual authorized by a covered entity or business associate that was made in "good faith," within the scope of such person's employment or an inadvertent disclosure by such an individual who otherwise has access to such information.[4]

The Statute

The HITECH Act applies to covered entities, as defined in the Health Information Portability and Accountability Act (HIPAA), which includes medical practices.[5] Additionally the HITECH Act utilizes the same definition for PHI as HIPAA:

> **Protected health information:** individually identifiable health information that is (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium.[6]

This is an extremely broad definition that encompasses names, contact information, and addresses, regardless of whether directly related to the patient's health or not.

The HITECH Act requires all HIPAA-covered entities, including medical practices, to notify each patient whose unsecured PHI has been or is reasonably believed by the practice to have been acquired, accessed, used, or disclosed as a result of an unsecured PHI breach.[7] It is important to note that the breach notification requirements only apply to unsecured PHI, which is unencrypted PHI. PHI is deemed "secure," pursuant to guidance issued by HHS on April 27, 2009, if it has been encrypted in the manner that the HIPAA Security Rule delineates.[8] This guidance recommends that PHI be rendered unreadable, unusable, and/or indecipherable by unauthorized individuals. Thus, practices that take measures to secure their PHI will not be subject to the notification requirements in the event of a breach, and the practice may avoid significant penalties, as set forth below.

The Notification Requirements

The notification, upon discovery of a breach, must be made "without unreasonable delay" and absolutely no later than sixty days following discovery.[9] A typical reason for practices delaying the notification may be that they are investigating the breach, but the HITECH Act requires that any investigation be conducted expeditiously in order to notify the affected patients as soon as possible.[10] Another exception to the sixty-day timeframe for notification is a request for delay by law enforcement.[11] A breach is discovered on the first day that it is known to the practice, including any employee of the practice, or that the practice should have known based upon reasonable diligence.[12] "Reasonable diligence" is defined as the "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances."[13] Consequently, it is vital that practices train their employees to report any suspicion of a breach immediately to the practice's administration.

The law enforcement notice delay provision permits a practice to delay the notification of the patients beyond the sixty-day timeframe only if requested by a law enforcement official. This

request may be made in order to avoid impeding a criminal investigation or causing damage to national security and must be provided to the practice in writing. Nonetheless, the practice is still required to document the length of the delay and the identity of the law enforcement official making the request.[14]

This could be a major undertaking for practices because they must notify the affected patients: (1) in writing; (2) by first class mail; and (3) send such notice to the last known address of the patient or to the next of kin if the patient is deceased and the practice knows that the patient is deceased.[15] A way to simplify this process would be to have patients authorize electronic notice for any breach notifications upon joining the practice. If the practice has provided the patient with such an opportunity prior to discovering a breach, electronic notification is permissible.[16] Where the contact information for the patient is out-of-date, substitute notice may be employed and must be provided as soon as reasonably possible after the practice learns that the contact information it has on file is insufficient.[17] If fewer than ten patients are affected, such substitute notice may include but is not limited to a telephone call, email, or, if there is a complete lack of current contact information, a posting on the practice's website.[18] In the event that the breach affects ten or more patients, substitute notice may include a conspicuous posting on the practice's website (if the practice has a website) for ninety days or an announcement in major print or broadcast media in the geographic areas where the affected patients reside. Practices should utilize both forms of substitute notice to ensure that the notification reaches all of the affected patients. This form of notice must include a toll-free phone number.[19] Notice on the website should be displayed on the homepage or on another page linked prominently from the homepage.[20] In contrast, if notice is provided via media, the type of media and the breadth of the geographic area reached by such media utilized will vary based upon the affected patients' residences. If the affected patients all reside in a single community, notification through the community's newspaper would suffice. If the affected patients reside all over a large area, such as patients of a practice with multiple offices, notification through a newspaper that covers the entire area or several papers may be necessary to fulfill the regulations' mandates. No matter what the circumstances are, it must be clear that the practice is only responsible to provide substitute notice in areas where it knows that affected patients reside.

If the practice believes that there may have been a possible PHI misuse, the practice may but is not obligated to provide quicker notice to the affected patient in addition to the mailing.[21] Additionally, if the affected patient is a minor or otherwise lacks legal capacity, notice to the minor's guardian and/or the personal representative of the incapacitated patient is sufficient.

If the breach affects more than 500 patients, the practice will be required to provide notice through the media in addition to individual notice. Irrespective of the number of patients affected, the HITECH Act requires the practice to notify the HHS Secretary of the breach, but the time for such notification varies depending on the number of individuals affected. For breaches involving fewer than 500 patients, the practice may submit notice of all breaches together in an annual log to the Secretary, but absolutely no later than sixty days after the calendar year's conclusion. For larger breaches, the notice must be provided to the Secretary at the same time that it is provided to the individual patients. Further, for breaches affecting more than 500 patients, the HITECH Act requires the Secretary to post the name of the practice on HHS' website.[22] The form for notification to the Secretary may be completed on HHS' website at http://transparency.cit.nih.gov/breach/index.cfm.

The notification itself must include the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PHI, but not the actual details, that were involved in the breach, including but not limited to the name, social security number, date of birth, home address, account number, diagnosis, and disability code;
- Any steps that the patients should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the practice is doing to investigate the breach, mitigate harm to the patients, and protect against any further breaches;
- Contact procedures for the patients to ask questions or learn additional information, including a toll-free telephone number, email address, website, or postal address.[23]

Additionally, the contents of the notice must be in plain language so that the layperson can easily understand what has occurred and the steps he or she can take to contact the practice. Overly technical details should be omitted.[24] Notice through the media should include the same details as individual notification.[25]

Some groups have written to HHS requesting that the HITECH Act be amended to require breach notification only if there is a significant risk of harm to the patients whose PHI has been breached.[26] While HHS may consider such an amendment, at this time all covered entities must abide fully by the breach notification requirements, regardless of the risk of harm to patients.

Administrative Requirements

The HITECH Act also outlines numerous administrative measures that covered entities must take to implement these new breach notification requirements. Practices must establish policies and procedures to be followed when discovering or reasonably suspecting a breach. It is important for the practice to ensure that employees are aware of these procedures, and sanctions must be utilized in the event that employees do not abide by these policies. The practice must also develop a complaint system by which affected patients may register complaints regarding the procedures established by the practice and/or a failure of the practice to follow its own rules. These administrative regulations are not optional.[27]

The Penalties

Practices will be sanctioned for failing to comply with the HITECH Act breach notification requirements.[28] The following chart simplifies these sanctions:

Nature of Violation	Range of Penalties	Maximum Penalty
Violation unknown or by exercising reasonable diligence would not have known	$100 for each violation, up to $25,000 for all identical violations in a calendar year	$1.5 million for all violations of this type
Violation due to reasonable cause and not willful neglect	$1,000 for each violation, up to $100,000 for all such violations in a calendar year	$1.5 million for all violations of this type
Violation due to willful neglect, if corrected within thirty days from knowledge of violation	$10,000 for each violation, up to $250,000 for all such violations in a calendar year	$1.5 million for all violations of this type
Violation due to willful neglect, not corrected	$50,000 for each violation, up to $1.5 million for all such violations during a calendar year	$1.5 million for all violations of this type

Conclusion and Recommendations

Every practice is required to take the steps outlined in this article when it has discovered a breach of unsecured patient PHI. It is also mandatory for practices to develop new policies and procedures and train their employees to implement these breach notification requirements. The HITECH Act has placed the burden on covered entities to demonstrate compliance with these provisions, and failure to do so may result in steep penalties for a practice.

There are measures that practices can take now to avoid having to abide by these requirements or, at the very least, lighten the load on themselves should a breach require compliance. Each practice should make every effort to secure their PHI in accordance with the HHS-outlined guidance.[29] Additionally, every practice should obtain authorization from their existing patients to use electronic notice to notify such patients if there is a future breach of their PHI. Concurrently, practices should get into the habit of acquiring the same permission from new patients as they join the practice. Electronic notice is much faster and cheaper than first class mail. Practices should also confirm all patients' contact information to ensure that they have a current address on file. Finally, for notification purposes as well as other uses, practices should develop a website. These recommendations will ease the burden on practices in the unfortunate occurrence of a PHI breach.

1 Health Information Technology for Economic and Clinical Health Act, § 13402, *codified* at 42 U.S.C. § 17932.
2 Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42740 (Aug. 24, 2009) (*codified* at 45 C.F.R. §§ 160 and 164).
3 HITECH Act § 13400(1)(A), codified at 42 U.S.C. 17921.
4 HITECH Act § 13400(1)(B), codified at 42 U.S.C. 17932(b).
5 Breach Notification for Unsecured PHI, 74 Fed. Reg. 42740.
6 Health Information Portability and Accountability Act, 45 C.F.R. 160.103.
7 Breach Notification for Unsecured PHI, 74 Fed. Reg. at 42749 (*codified* at 45 C.F.R. § 164.04(a)(1)).
8 Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009, 74 Fed. Reg. 19006 (Apr. 27, 2009) (*codified* at 45 C.F.R. §§ 160 and 164).
9 HITECH Act § 13402(d)(1), *codified* at 42 U.S.C. 17932(d)(1).
10 Breach Notification for Unsecured PHI, 74 Fed. Reg. at 42749.
11 HITECH Act § 13402(g), *codified* at 42 U.S.C. 17932(g).
12 HITECH Act § 13402(c), *codified* at 42 U.S.C. 17932(c).
13 Breach Notification for Unsecured PHI, 74 Fed. Reg. at 42749 (*codified* at 45 C.F.R. § 164.404(a)(2)).
14 *Id*. at 42755 (*codified* at 45 C.F.R. § 164.412).
15 HITECH Act, § 13402(e)(1), *codified* at 42 U.S.C. 17932(e)(1).
16 *Id*.
17 *Id*.
18 Breach Notification for Unsecured PHI, 74 Fed. Reg. at 42751(*codified* at 45 C.F.R. § 164.404(d)(2)(i)).
19 *Id*.
20 *Id*.
21 HITECH Act § 13402(e)(1)(C), *codified* at 42 U.S.C. 17932(e)(1)(C).
22 *Id*.
23 HITECH Act § 13402(f), *codified* at 42 U.S.C. 17932(f).
24 Breach Notification for Unsecured PHI, 74 Fed. Reg. at 42750.
25 *Id*. at 42752.
26 Provider, Industry Groups Support No-Harm Provision in Data Breach Rule, HEALTH LAW REPORTER, Oct. 29, 2009, at 1438-39.
27 Breach Notification for Unsecured PHI, 74 Fed. Reg. at 42755 (*codified* at 45 C.F.R. § 164.530).
28 HHS has confirmed that it will not impose sanctions for failure to comply with the notification requirements prior to February 22, 2010, as it realizes that practices may need time to develop policies and procedures for implementation.
29 *See supra* text accompanying note 8.