2011 Issue 4

www.ober.com

Breach Reporting Plans: Practical Preparation for the (Almost) Inevitable Breach

By: James B. Wieland and Joshua J. Freemire

If there is one aspect of the HITECH Act amendments to the HIPAA privacy rule that has had a major impact on the health care provider community and its business associates, it is the so called "Breach Notification Rule." The rule requires that covered entities (and their business associates) report breaches of unsecured protected health information to both the subject individuals and to the Secretary of Health and Human Services, unless the breach falls within a narrow statutory exception or, at least at present, the breach fails to reach a controversial "harm threshold." (*For a more detailed discussion of the Breach Notification Rule, and its detailed reporting requirements, see Jim and Josh's article, "HITECH Act Breach Notification Rule Now in Effect, But No Sanctions Apply Until 2010."*) While this rule caused quite a stir in the HIPAA community, it is also important to remember that it represents only half of the puzzle – in many states, local data breach notification laws impose even stricter requirements and shorter time lines.

As Dr. David Brailer, President Bush's appointee as the National Coordinator for Health Information Technology noted in the May 30, 2011, New York Times article, "Breaches Lead to Push to Protect Medical Data," securing health information technology poses unique challenges. "Break-ins and hacks," Dr. Brailer explained, "are unfortunately going to be a part of the landscape." The authors' experience indicates that the source of breaches may be equally likely to be human error by work force members, if not knowing violation of the HIPAA rules. While the health care world may not be divided into those entities that have had a reportable breach and those that just haven't had one yet, taking practical steps in anticipation of a breach is advisable, particularly given the short time to respond.

"Just the Facts, Ma'am"

The first step in any breach response preparation is to ensure that workforce education and training are both sufficient and current. All members of the workforce must know how to identify a possible breach and whom within the organization to notify. In most situations, a workforce member is not trained to determine whether a breach has taken place. That is a job for the privacy officer and, possibly, legal counsel. Given the short timelines provided in the Breach Notification Rule, however, it is essential that frontline employees know to act quickly when they believe they may have discovered a breach. Similarly, it is important that internal compliance procedures ensure that workforce level breach reports are not "lost in the shuffle" or "back-burnered."

HIPAA privacy policies and procedures should specifically deal with this topic, but given the importance of the topic and the importance of prompt notification by workforce members, a simple reminder to the workforce may be useful. Below is a draft reminder notice, but providers should always consider the unique risks that they face in educating their workforce. Reminders should, to the best extent possible, remind employees of the risks inherent in situations they actually face.

Illustrative Example of Workforce Reminder

HIPAA REMINDER:
REPORT BREACHES OF SECURITY TO THE PRIVACY OFFICER IMMEDIATELY

As you know, the company has adopted HIPAA Policies and Procedures to help ensure our compliance with this important legal requirement. Among our duties to safeguard protected heath information with which we are entrusted is our duty to report a breach of the security of that information, promptly, to the affected individuals so that they can take steps to protect themselves from misuse of that information.

This is a reminder that provides a simplified overview of these important requirements. If you have questions, please review our policy and procedure [ADD A CITATION] or contact the Privacy Officer [ADD NAME AND CONTACT INFORMATION].

"Protected Health Information" is information in oral, paper or in electronic form that is created by a health care provider or a health plan and that relates to the past, present, or future physical or mental health of an individual; the provision of health care to an individual; or the past present or future payment for the provision of health care to an individual if that information identifies the individual or if it is possible to indentify the individual from the information.

A *"possible breach"* means that someone accesses or uses a patient's protected health information, or acquires or discloses a patient's protected health information, when they shouldn't or that protected health information may be exposed to unauthorized access, whether by a member of our workforce or by a third party.

Some examples of a possible breach would be (i) sending an email containing Protected Health Information that is not encrypted to an incorrect email address; (ii) leaving paper files that contain Protected Health Information in a public area of the company, especially if there is evidence that those files have been looked at by an unauthorized individual; or (iii) loss, including theft, of a paper file or a computer or other electronic storage device containing unencrypted Protected Health Information.

Workforce members should not attempt to determine whether a possible breach as described above requires responsive action under HIPAA. Such determinations will be made by the Privacy Officer in consultation with the Firm's General Counsel.

Workforce members have the vital, "front-line" role to be alert for possible breaches and to report all known or suspected breaches immediately to the Firm's Privacy Officer. The contact information for our Privacy Officer is _____.

"The Buck Stops... Where?"

Depending on the size and geographic dispersion of the company, it may be advisable to designate a breach response team in advance of a breach. Such a team should include not only the privacy officer, but legal counsel and a representative of senior management. All team members should be familiar with the issues and the rules and be authorized to take action. Having a member of senior management on the team is important, given the potential reputational damage that a breach may bring upon the company and the potential costs of investigating and notifying subject individuals. A senior management-level team member will have the authority necessary to make rapid decisions with regard to the need for additional investigation or retention of outside counsel, and can authorize immediate steps to mitigate potential harm from both the breach itself and the attendant public relations issues.

"What a State You're In!"

Actually, it's the state the individual whose protected health information was subject to the breach is in that counts. Since nearly every state has a consumer protection law that requires notification of individuals if their personal information, such as social security number, driver's license number, or banking information is exposed to unauthorized access, the breach response team will need to also be aware of relevant state law requirements. Though many state laws impose requirements and deadlines that are generally similar to those of HIPAA, some (such as California) have imposed significantly shorter notification deadlines and mandatory civil penalties for failures to timely notify. Like the HIPAA breach notification, state law notification requirements do not typically apply to information that is encrypted, but each state's laws must be considered, since there are significant variations.

Files with protected health information typically also include personal information, especially social security numbers, and required state-level notifications should be coordinated with any federal notification. Usually, one notice, if properly drafted, will fulfill both state and federal requirements. Since, generally, it is the state of the subject individual, not the state of the company facility that governs the application of state laws, the breach notification team should be familiar, at a minimum, with requirements of the state laws for the states that provide the majority of the customers or patients.

One of the first questions that the breach team should ask, if a breach is confirmed, is where the subject individuals lived. Once states of residence have been identified, the team can determine whether the breach in question involved the types of data covered by the applicable state law, and what additional requirements, if any, the state law mandates for the notification process.

"Encrypt Early, Encrypt Often"

The costs of encryption have decreased dramatically in recent years. If there is a universal vaccine against reportable breaches under HIPAA (and under most state consumer protection laws) it is encryption of the protected information. The HIPAA breach rules specifically exclude breaches of data that is encrypted in accordance with the Guidance and Request for Information published by the Secretary of HHS in early 2009 [PDF]. Providers can spare themselves a great deal of potential work (and spare their patients and customers a great deal of worry) by ensuring that all PHI and state breach law covered data is, to the greatest extent possible, stored and transmitted in encrypted form. The breach response team should know where data is encrypted and where it is not – if a laptop is stolen, knowing that its data was encrypted could spare the organization from sending thousands of breach notifications and enduring a responsive HHS OCR investigation, to say nothing of the articles in the local newspaper.

"Don't Spare the Horses... or the Trees"

While many breaches are straightforward, some, particularly those involving the loss of paper or electronic records of numerous individuals, are not. Intense investigation, started as soon as the breach has been identified, serves multiple functions. An aggressive (and appropriately documented) investigation may lead to important and relevant information about the breach. It may also assist the entity, in case complete information is not discovered within the 60-day time limit, to formulate appropriate interim notices. Finally, an aggressive and well-documented investigation is an entity's best hope, especially in the case of a large breach, of avoiding extensive government scrutiny and, if necessary, justifying existing policies and procedures, and explaining the mitigation and notification actions that have already been undertaken. Remember, when it comes to government compliance enforcement, we all live in the "Show Me" state.

"It's Who You Know"

While a great deal of ink has been spilled with regard to sophisticated foreign cabals who engineer complicated computer hacks to steal personal information, the vast majority of reported major breaches stem from simple human error. Records are tossed in the dumpster, a file is left on a train, curious employees access records about friends or a local celebrity when they have no reason to do so. These are common, but not complex, problems. It can be too easy to fear the great unknown when perhaps the greatest compliance threat most entities face is posed by their own workforce members. Education and vigilance are the answer to these "every-day" threats.

The breach response team can, and should, play an active role in employee education and general compliance activities. By discussing the danger of breaches (and their potential costs to the organization) the breach response team can encourage generalized workforce vigilance to the problem, particularly if a representative of senior management is a visible part of the team. By making themselves and their role well-known to workforce members, the breach response team can help ensure that they will receive timely notice of potential breaches. Finally, by sharing their detailed knowledge of the requirements of the applicable federal and state laws, the breach response team can help reassure workforce members that breaches are nothing to panic about – if they can't always be avoided, they can certainly be quickly, comprehensively, and professionally addressed.