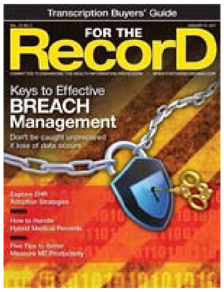
January 31, 2011


Transcription Buyers' Guide
FOR THE RecorD
Keys to Effective BREACH Management
Don't be caught unprepared if loss of data occurs

Keys to Effective Breach Management
By Lisa A. Eramo
For The Record
Vol. 23 No. 2 P. 14

Being thorough is priority No. 1 when establishing a policy that takes the guesswork out of managing disclosures.

The question isn't whether you'll have a breach, it's when. And when you do, your organization better have a plan in place to handle it.

"Every organization will experience breaches," says Ali Pabrai, CISSP, CSCS, CEO of ecfirst, Inc, which specializes in delivering IT services to the healthcare and financial industries. "When you experience a breach, that's not the time to discover you have a procedure that doesn't work. You don't want to be scrambling to figure out what to do. You just won't have the time to go through that."

The notification process under the HITECH Act can be extremely labor intensive and costly, says Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA, director of practice leadership at the AHIMA. "Breach notification requires a lot of expenditures. It takes a lot of money to respond," he says.

The average cost of a data breach is $204 per compromised customer or patient record, according to a January 2010 study conducted by the Ponemon Institute, which performs independent research on privacy, data protection, and information security. This includes $144 in indirect costs and $60 in direct costs. The cost per record of a data breach involving a laptop computer or other mobile device is $225.

Perhaps far more damaging in the long run is the fact that breaches could cost organizations their reputations. Poorly executed or confusing data breach response efforts can lead to other negative consequences, such as patients who seek care elsewhere, says Rhodes.

"To come out and say that you have a breach can be really detrimental," he says. Even in small communities, patients who are concerned about the privacy and security of their health information can avoid seeking care from a provider that encountered a breach and simply drive up the road to another provider with a better reputation for health information security, he adds.

In an April 2008 study conducted by the Ponemon Institute, 63% of survey respondents said notification letters they received offered no direction on the steps they should take to protect their personal information. As a result, 31% said they terminated their relationship with the organization, and 57% said they lost trust and confidence in the organization.

Acknowledge the Breach
When thinking about breaches—particularly those involving unsecured protected health information (PHI)—the first step is to simply acknowledge the breach, says Dennis Melamed, president of Melamedia, LLC, a publishing and consulting company in Alexandria, Va. "Don't be in denial that something happened. You can't ignore it," he says.

Identity thieves move very quickly, either using PHI or selling it, says Rhodes. That's why it's important for organizations to take every threat seriously, react promptly, and identify the source of the breach.

"One of the things that always amazes me is that organizations seem to be taken off guard," he says. Rather than wait for a breach to occur and then devise a process for dealing with it, organizations should establish a team that can recognize the breach and immediately trigger a response, says Rhodes. That team should include HIM, the privacy officer, information systems, IT security, risk management/legal, physical security,

admitting staff, nurse auditors, compliance, clinicians, and administration.

Organizations may also want to name an internal breach investigator who can manage the breach investigation process from the beginning, says Rhodes. “He or she can lead the incident response team and can become the sole external spokesperson for the organization. He or she oversees completion of the risk assessment and manages all of the breach notification documentation,” he says.

Perform a Risk Assessment
After identifying a breach, organizations must perform a thorough risk assessment to determine whether the breach could be harmful to the affected individual(s). If the breach involves unsecured PHI—and the covered entity (CE) or business associate (BA) deems the breach harmful—the CE or the BA is obligated to follow HITECH requirements for breach notification. The Office for Civil Rights (OCR) defines a breach in its interim final rule (available at http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf) as an event that “poses a significant risk of financial, reputational, or other harm to the individual.”
“This is controversial,” says Melamed. “Some of the references in the interim rule suggest that you’re almost always going to have harm. If it’s more than 500 [individuals], there tends to be a presumption of harm.”

However, the number of patients is not the only factor to consider, adds Melamed. “It’s also important to remember that CEs often have responsibilities to correct and mitigate breaches that do not reach the 500-patient threshold. In fact, that’s where you are going to face these issues on a more day-to-day basis,” he says.

The OCR states that CEs and BAs should take the following into consideration when determining harm:

• Who impermissibly used the PHI or to whom was it impermissibly disclosed? For example, if the data were impermissibly disclosed to another entity governed by HIPAA, there may be less risk of harm to the affected individual(s). If the data are disclosed to an entity or a person who isn’t required to follow HIPAA, there may be more of a risk.

• Was the PHI impermissibly disclosed but then returned prior to it being accessed for an improper purpose? For example, if a laptop is stolen and then recovered and a forensic analysis shows that its information was not opened, altered, transferred, or otherwise compromised, this breach may not pose a significant risk. However, the OCR states, “We do not consider it reasonable to delay breach notification based on the hope that the computer will be recovered.”

• What is the type and amount of PHI impermissibly used or disclosed? The OCR states, “If the nature of the protected health information does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach.” For example, if a CE improperly discloses an individual’s name and the fact that he or she received services from a hospital, this is not a breach. However, if the information includes the type of services (eg, oncology services), the specific type of facility (eg, a substance abuse treatment facility), or other valuable information (eg, Social Security number, account number, maiden name), there is likely a great risk for the affected individual(s).

Notification Responsibilities
The OCR expects organizations to react quickly upon discovery of a breach that could cause harm, says Melamed. “OCR makes it pretty clear that when the breach hits their public website, this should be the last place that anybody hears about it. They want covered entities to be well on their way to correcting this as they report it,” he adds.
What does this mean for organizations from a legal perspective? According to the OCR interim final rule, CEs must notify affected patients “without unreasonable delay” and no later than 60 calendar days after the date the breach was discovered. This requirement is mandatory regardless of the number of individuals affected by the breach.

However, breaches affecting 500 or more individuals require notice to the secretary of Health and Human Services (HHS) and prominent media outlets serving a state or a jurisdiction (eg, a major general interest newspaper with a daily circulation throughout the entire state). Breaches affecting fewer than 500 individuals require annual notice to the HHS secretary 60 days after the end of each calendar year.

Organizations should note that although HITECH specifies a timeline of 60 calendar days, several state regulations are much stricter, says Pabrai. In California, for example, organizations must notify state agencies within five days. State regulations may also be stricter in terms of notification thresholds and enforcement. “You must notify state agencies regardless of whether the breach affects five or 500 individuals,” Pabrai adds.
The OCR says breach notices to individuals should include the following:

• a brief description of what happened, including the date of the breach and the date of discovery, if known;

• a description of the types of unsecured PHI that were involved in the breach (eg, name, date of birth, address) (CEs should not include the actual PHI that was breached.);

- any steps individuals should take to protect themselves from potential harm resulting from the breach;

- a brief description of what the CE is doing to investigate the breach, mitigate damages, and prevent future breaches; and

- whom to contact with questions or for more information.

When an organization can't determine what specific information was breached but it has a strong suspicion regarding the type of data, it's best to be open and honest with patients about the information that may have been compromised, says Pabrai. It's a good idea to consider providing patients with a summary of what you send to the OCR on its breach notification form, he adds.

The OCR interim final rule also specifies methods for notification, including what to do when the organization doesn't have sufficient contact information, when the information is out of date, and when the affected individual(s) is deceased.

The AHIMA provides a model breach letter that incorporates all the requirements outlined in the OCR interim final rule at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_045987.pdf.

Don't forget about BAs and the role they may play in the breach notification process, says Melamed. CEs need to know if and when the BA will be responsible for breach notification. This will depend on the specific circumstances of the breach and the contracts that exist between the CE and the BA, he says.

"Although the presumption is that the covered entity is primarily responsible for breaches that occur, in my mind, I don't think OCR cares [which entity actually notifies individuals] as long as the individuals are told in a timely fashion and [CEs or BAs] take action to mitigate, correct, and notify," Melamed notes. "The question among healthcare executives is who is going to be responsible to pay for this."

Mitigate
Organizations must clearly articulate what steps they're taking to protect a person's reputation and prevent negative financial consequences, says Pabrai. This often includes providing free credit monitoring services to affected individuals.

According to the OCR, the sooner an organization notifies an individual that his or her PHI may have been compromised, the more easily the individual may be able to mitigate any embarrassment that exposure of sensitive medical information may cause.

Draft Updated Policies and Procedures
Organizations should develop a breach management policy that incorporates each of these steps and further establish a comprehensive incident response plan, says Pabrai. HIM professionals should work closely with IT to ensure that all policies and procedures related to breach management reflect HITECH requirements.

Pabrai says an effective breach management policy should include the following three elements:

1. Discovery: How will the organization identify that a breach has occurred? Is the organization taking proactive steps to detect breaches? Have security controls been deployed to alert someone to missing laptops or devices?

The bottom line is that organizations must be able to determine as quickly as possible when the breach occurred. "If there is a big gap between the date of the breach and the date of the discovery of the breach, that's a signal to federal and state authorities that somehow the organization does not have the capabilities in place to determine on a timely basis that a breach has occurred," says Pabrai. "It's important that the discovery process take into account the type of security controls the organization may have implemented to discover breaches on a timely basis."

For example, organizations can run weekly reports to identify laptops that haven't been accessed for five to seven business days. "An alert is triggered and then a verification can be performed with the department regarding the state of the device to see whether it has been lost or stolen," says Pabrai.

2. Reporting: How will the organization collect information about the breach? "There's a lot of specific information that OCR is expecting with respect to a breach that an organization may experience," says Pabrai. "That's the type of reporting capabilities that an organization should be managing, regardless of whether they have to report the incident to OCR or not."

3. Notification: Identify ahead of time which entities (eg, patients, the media, state or federal agencies) require notification in certain circumstances and the timeline for those notifications, says Pabrai. Also identify contact information for each of these entities so the information is easy to reference when a breach occurs.

Focus on Portable Media
Organizations should place a primary focus on portable media because of its tendency to contribute to breaches.

“One of the easiest things to do is to secure your laptops and encrypt them,” says Melamed. “People who hold onto PHI need to know they need to take care of it so people don’t steal it or lose it. You need to take a more serious approach to the loss of data. It’s about literally physically securing the data.”
However, before an organization goes through the process of encryption, it must complete an asset inventory, says Pabrai.

Creating an asset inventory can be a challenge, and many hospitals don’t have an accurate count of their portable devices, including how many exist, where they exist (in which departments), and who owns them (who makes decisions regarding what information is stored on them and how that information is used).

Pabrai says it’s important to identify an individual in each department who can specify all portable devices in use and be sure they are included in the inventory.

“Without this [inventory], it will be impossible to complete an all-encompassing encryption process,” he says. “You may miss out on certain devices and then, if those devices are lost or stolen, that increases risk to the organization.”

Don’t forget about employee-owned devices either, says Pabrai. Organizations should establish policies approved by the CEO or the president that ban employees from being able to store PHI on their personal devices. Post the policy on the intranet and provide weekly reminders so employees know the organization’s stance on the use of portable devices, he adds.

Some hospitals have opted to disable USB ports to deter employees from downloading and uploading PHI, says Rhodes.

Stay Involved
Experts say the best way in which HIM professionals can deter breaches is to simply stay involved in the breach management process. Consider the following ways you can contribute to your organization’s compliance:

• **Serve as a resource for patients:** If a patient suspects he or she may be the victim of medical identity theft, listen to his or her concerns, provide resources, and investigate whether a breach may have occurred that led to the theft, says Rhodes.

Likewise, if an audit trail reveals suspicious activity on a patient’s account, don’t hesitate to call him or her. “A lot of people are afraid to call patients, but in this day and age, you can’t afford to not do this,” Rhodes says. “If the facility suspects something, it’s OK to call the consumer and inquire about potentially suspicious activity. It gives you an opportunity to work directly with the consumer and shows that you are paying attention.”

• **Advocate for better access-level controls:** Employees should have access only to the information they need to perform their job, says Rhodes. Be cognizant of individuals who are promoted or transferred to a new department because their access level may need to change, he adds.

For new employees, take the time to think through the specific information to which they need access rather than using a blanket access for the department in which they work, says Rhodes. When someone leaves the organization, terminate access immediately.

• **Advocate for updated security safeguards:** “A lot of the security safeguards that were good five years ago or even three years ago may not be sufficient now. There are new threats, so you need to review what your threats and vulnerabilities are,” says Rhodes. “Hospitals need stronger safeguards so they know the exact time and date; they know how much information was taken. They should be able to know whether it was someone internally or someone from the outside.”

• **Hire a data integrity specialist:** Although many individuals in this role were originally hired during EHR rollouts to ensure that providers and others were accurately entering data and avoiding duplicate records, they are now increasingly focusing on unusual data activity in the record, says Rhodes.

• **Review audit logs:** Organizations should periodically review audit logs to look for any suspicious actions or unusual amounts of data activity and immediately review the logs when a breach is suspected, says Melamed. Pay close attention to the following:

— Break the glass” data access. Audit this information regularly to determine who accessed the data and why.

— Multiple unsuccessful attempts to access a device. Disable accounts that fit these criteria and require staff members to contact the IT help desk to reactivate the device, says Pabrai.

— EHR-generated red flags, which some vendors can provide.

• **Create a robust training program:** Make sure employees understand why they're protecting patient data. "Patient data is like money. You don't leave it out or unattended; you take care of it. You will track PHI pretty carefully when you think of it that way," says Melamed.

Pabrai recommends a proactive audit policy in which you randomly audit information accessed for five patients and five employees. This should occur at least quarterly to ensure the effectiveness of policies, procedures, and education.

— Lisa A. Eramo is a freelance writer and editor in Cranston, R.I., who specializes in healthcare regulatory topics, HIM, and medical coding.

Great Valley Publishing Co., Inc.
3801 Schuykill Road
Spring City, PA 19475