Sounding the Alarm: Knowing When to Notify Patients of a Data Breach Can Be Unclear

by **Chris Dimick**

Forty-four states require organizations to alert customers and employees when data breaches occur. But ambiguity in the laws requires organizations to be capable of making good decisions on their own.

The laptop was missing.

Previously stationed in the EEG department of NorthShore University HealthSystem, the laptop had been connected to equipment used by staff to treat patients. Just who took the laptop from the Evanston, IL-based facility—an employee, patient, or visitor—was not known.

What was known was that 250 patients had personal information stored on the machine, including their names and Social Security numbers.

NorthShore's chief privacy officer and director of HIM is Teresa Bunsen, RHIA. When she was notified of the theft, her thoughts raced to the missing patient information. The laptop was not encrypted, leaving sensitive information exposed to potential theft.

It was clearly and officially a breach that threatened patient privacy, and Bunsen sounded the alarm. That triggered an investigation and a breach notification letter sent to the 250 patients.

Most providers operate under state laws that require them to alert patients and employees if their data were involved in a privacy or security breach. However, few of the laws are specific, which can leave privacy officers wondering just how and when to send a notification.

Send too early, and a false alarm could cause patients unnecessary worry and damage the organization's credibility. Wait too long, and identity theft and state fines will make a bad situation worse. Establishing policies, procedures, an operations team, and staff training helps organizations make the best choices when they find themselves in the middle of a breach situation.

What Constitutes a Breach?

Data breaches are serious matters for both patients and healthcare facilities. The threat of unauthorized record access strikes at the core of a facility's promise to keep information confidential. When information is breached, quickly notifying patients or employees can greatly improve their chances of combating harm from identity theft.

Currently 44 states have data breach notification laws, which require stewards of personal information, such as healthcare facilities, to notify customers and employees if their personal health information is improperly accessed or stolen. California was the pioneer in enacting breach laws in 2002.

California again has come into the national spotlight with two new breach notification laws that took effect January 1. The laws sharpen the requirements—and teeth—of the state's breach legislation.

California's new laws require healthcare organizations to report all unauthorized access to affected patients and to the newly created California Office of Health Information Integrity within five days of discovery. The laws also dramatically increase fines placed on facilities for unauthorized personal information disclosures. (For more, see sidebar on the following page.)

Just what triggers a breach notification varies from state to state, says Alan Wernick, Esq., an attorney with Wernick and Associates, LTD, based in Northbrook, IL.

In many states, including Illinois, law establishes that a breach occurs when exposed patient information contains first name or first initial and last name combined with either a Social Security number, driver's license number, account number, or credit or debit card number. The incident is only considered a breach if the information is not encrypted, a common element of data breach statutes in most states. For these reasons, NorthShore's stolen laptop clearly classified as a breach under the law.

Other state laws include additional data elements, or "personal identifiable information" (PII), that if breached require notification, such as medical information, Medicaid account numbers, or insurance policy numbers. In California, medical and health insurance information are specifically covered in breach laws. These terms were added in 2007.

But not all state laws contain this specificity. In those states, if a patient record containing sensitive information was released and didn't contain the above-mentioned information—such as Social Security number or bank account information—the facility legally would not be required to notify the patient. However, many facilities do notify patients, because they feel ethically it is the right thing to do, says Reece Hirsch, partner with national legal firm Sonnenschein Nath & Rosenthal, LLP.

Some laws are open to interpretation. Many states have a standard written into breach law that facilities with a "reasonable belief" that unauthorized access to personal information has occurred must notify patients. That wording can leave facilities with a tough decision to make.

For example, a classic breach situation is a laptop stolen from the front seat of a car, says Hirsch. The laptop contains medical information and Social Security numbers, but there is no clear indication that the thief was after the data.

The thief "might not even access that data, depending on how it is stored on the laptop," says Hirsch. "But, in most cases in my experience, when companies are faced with making that kind of judgment call, they tend to err on the side of caution and notify, because the consequences of not notifying can be pretty severe."

California's New Laws

After a series of high-profile breaches of celebrities' health records in California, including those of Governor Arnold Schwarzenegger's wife, Maria Shriver, the state passed new legislation that gives sharper teeth to breach laws.

California laws AB 211 and SB 541 went into effect January 1. They add significant changes to what constitutes a privacy breach and how long facilities have to notify victims. The biggest change: more fines and a shift to preventing unauthorized access. Organizations can now face up to $250,000 in fines for allowing a data breach.

The steep hike in fines was no accident, says Cassi Birnbaum, RHIA, CPHQ, the director of health information and privacy officer at Rady's Children's Hospital of San Diego. "That was well intentioned from a state perspective, because they wanted to make sure that people would take this seriously," she says.

New Focus on Unauthorized Access

The new laws say that healthcare providers must take steps to prevent "unauthorized access" to patient information, not just "unlawful" access as the law previously read. Facilities are now liable every time an employee snoops through a patient's files. Both the healthcare organization and individual can be fined up to $25,000 for each patient whose information was accessed, used, or disclosed in an unauthorized manner.

Organizations that negligently disclose patient information now face fines from $2,500 to $25,000 per violation. Individuals or organizations that use patient information for financial gain face fines of up to $250,000 per violation. The laws also make it easier for patients to sue when their information is breached, even if they did not suffer actual harm.

Previous state law required organizations to report breaches to the patients affected. The new laws require that organizations also report breaches to the California Office of Health Information Integrity, a newly formed office within the California Health and Human Services Agency.

Healthcare organizations now have five days after discovery of a breach to notify both parties. They will be fined $100 for each day they are late in reporting.

Early Reactions

The minimum necessary rule in HIPAA already bans unauthorized accesses to patient records, so the conduct discussed in the new California rules is arguably unnecessary, Hirsch says. “But, because this is viewed as a particularly sensitive area, California has decided to go further and create specific sanctions, put some real teeth in this,” he says. “This definitely raises the bar considerably and would cause organizations to take an even more rigorous approach to enforcing access controls.”

Healthcare facilities are worried about having to report incidents to the state, mainly because even the most diligent and secure organizations are going to have some instances of unauthorized access, Hirsch says. “Human curiosity is what it is…it is not right, but it does happen time and again,” he says. “It is going to be interesting to see how the California Department of Health responds when they receive these reports of unauthorized access, because this is something that to one degree or another is almost unavoidable in many organizations.”

Although the new laws will put pressure on compliance and other hospital departments to implement stricter record monitoring, auditing, and other security processes, Birnbaum says she can see why the laws were passed.

“I really think that the state was frustrated, and there is a perception out there from a consumer standpoint that we weren’t doing enough, we weren’t taking the law seriously enough,” she says. “And so that is why we are now faced with some really ominous teeth in already over-the-top regulations for confidentiality and privacy.”

Other States to Follow Suit?

Even though 44 states followed California’s initial lead in passing breach notification laws, Hirsch doesn’t feel the new California laws will also be adopted by other states. “I think this was driven by a few high-profile incidents, and I don’t know that there is the same pressing need to fill a gap as there was with state security breach notification,” he says.

However, Wernick sees the potential for a ripple effect, noting that the instances of snooping are not isolated to celebrities in California. “What we have seen happen in California…is not unique to California—they are problems that affect people in just about any state,” Wernick says. “Until there are better controls and a better way to deal with these types of data breaches, then there is going to be continuing legislative efforts to deal with this.”

When to Notify?

California law requires facilities to give notice within five days of discovering a breach; other state laws are more ambiguous. In Illinois, the law states that notification must be made in the “most expedient time possible and without unreasonable delay.” The organization may delay their notification, however, if “appropriate” law enforcement officials deem it necessary to conduct their investigation into the incident.

One of the most common mistakes in responding to a breach is failing to understand one’s legal obligations, Hirsch says.

“You need to sensitize your organization to what constitutes a breach, and when one occurs, whether it is the theft of a laptop or a hacking incident, employees need to know that it is a serious matter that needs to get reported up the chain of command very promptly,” he says.

The point of notification is to help patients prevent financial fraud and identity theft. Because those crimes can happen very quickly, it is best for facilities to promptly notify patients after an incident is determined a true breach.

"Usually there isn't a set time frame, but it is essentially as soon as possible," Hirsch says.

However, facilities should balance prompt notification with sufficient review of the situation. When any privacy or security incident occurs, privacy officers should not overreact and immediately make information public about the incident. Since some state laws do not specify a certain time frame for reporting, there is room to conduct a thorough in-house investigation to confirm whether there was actually a breach.

Even when there is a time limit, it is typically long enough—in some states 45 days—to sort out a situation. A proper investigation should always come before a notification letter, Wernick says. An organization has an "obligation to investigate [and] find out what the nature of the breach is" in order to even know who to notify, he states.

A facility should be sure notification is required before proceeding. Once a letter has been sent, the organization can't "unring the bell" if further investigation determines that no notification was lawfully deemed necessary, Hirsch says.

Be Prepared

For an organization to effectively respond to a breach it must be organized in advance, Wernick says. He recommends that organizations maintain an incident response team to respond to data breaches. The team can include legal, compliance, IT, and public relations representatives, and it should meet regularly to discuss changes in law and review breach notification procedures.

If a major breach does occur, a facility won't have time to figure out who should send the letters and who will staff a breach hotline number. All that needs to be determined beforehand, Hirsch says.

Smart organizations will take a play from their own book, Wernick says, and practice preventive legal measures in addition to preventive medicine. They should establish a tree-of-command for breach emergencies and practice how to handle a breach.

In the area of data breach and data privacy, hospitals that practice preventive legal measures have better legal health than those who don't, Wernick says.

Raising Employee Awareness

Training employees about the seriousness of a breach is important, Hirsch says. "One of the worst situations is when an employee knows of a breach, like the theft of a laptop, and doesn't report it immediately, and then it comes to the attention of the legal and compliance department a few weeks or month later," he says. "At that point you have had constructive knowledge of the breach for a month, and you were required by law to notify as soon as possible. So you have already basically violated the law."

Late notification will not sit well with patients, either. If identity theft had occurred, those patients will have been wondering who to point their fingers at for a month. It is reasonable to believe that when they get a notification letter after the damage is done, their next call will be to their attorney, Hirsch says.

Educating staff is an organization's biggest challenge when it comes to preparing for breach events, Wernick says.

When a laptop disappears, hospital employees may focus initially on replacing it in order to keep operations going smoothly. This was the case at NorthShore, where EEG department employees first contacted IT, not the privacy officer.

Replacing the equipment "tended to be the first thing people thought of . . . not the patient information that was likely lost along with the equipment," says Bunsen. "That was an eye opener," she says—that she still needed to get out there and continue educating staff that they must think about that loss of patient information, not just the loss of equipment.

NorthShore's Story

Breach education includes stressing the urgency of some practical steps, such as enacting policies that all facility laptops be encrypted to prevent access to their contents if they are stolen or lost.

That was a valuable lesson NorthShore learned the hard way. Encrypting all of the facility's laptops was on a to-do list, but the task didn't get done before the EEG laptop disappeared in summer 2007.

Once she learned of the loss, Bunsen quickly joined the facility's IS and compliance departments to investigate the incident. Bunsen had previously dealt only with small breaches affecting one patient; the missing laptop was the biggest situation she had faced in her eight years with NorthShore.

Once the EEG department pulled backup logs, staff were able to determine exactly which patients had information stored on the laptop. Part of that information was the patient's Social Security numbers, which Bunsen knew warranted a breach notification due to Illinois law. A letter was promptly sent to the patients involved, explaining the situation and how they could place a fraud alert with their credit reporting agencies.

Bunsen provided her office number on the letter, and she fielded a few calls from concerned patients. However, nothing negative ever came from the breach, Bunsen says.

Though an unwanted situation, some good has come from the incident at NorthShore.

The breach prompted the organization to immediately require encryption of all laptops. If a similar incident were to happen now, the theft would not put patient information at risk, Bunsen says. "It certainly was something that we wanted to do to safeguard information [beforehand]," she says. "But with having an incident, it definitely brought that project to the forefront."

Resources

More information on preventing and mitigating data breaches and identity theft may be found in the following *Journal* articles:

"Connectivity, Privacy, and Liabilities," April 2007 (vol. 78, no. 4)

"Data Theft and State Law," November–December 2006 (vol. 77, no. 10)

"How to React to a Security Incident," January 2008 (vol. 79, no. 1)

"Mitigating Medical Identity Theft," July 2008 (vol. 79, no. 7)

"Raising Awareness of Medical Identity Theft," October 2008 (vol. 79, no. 10)

"Securing Portable Devices," January 2009 (vol. 80, no. 1)

Chris Dimick (chris.dimick@ahima.org) is staff writer at the *Journal of AHIMA*.

Article citation:
Dimick, Chris. "Sounding the Alarm: Knowing When to Notify Patients of a Data Breach Can Be Unclear" *Journal of AHIMA* 80, no.2 (February 2009): 20-24.