Taking Action to Prevent Identity Theft in Assisted Living Facilities

Bob Spence

While technology enables quick and easy communication and documentation of information, it also can cause problems for organizations such as assisted living facilities that have personal information about their residents stored electronically. One of the most serious problems involves security breaches that result in or create a risk for identity theft.

According to Reece Hirsch, a Partner in Sonnenschein Nath & Rosenthal LLP, and speaker at a recent Atlantic Information Services audioconference on identity theft in health care, this problem is more than a legal concern. "How you respond to a security breach goes straight to the heart of your relationship with your customers," Hirsch said. In fact, he added, a "botched" response to a breach can lead to damaged customer trust, bad press and public relations, negative impact on stock prices, regulatory action, and even class action litigation.

People typically don't think of identity theft as being a problem in health care. However, Hirsch noted that a growing number of such instances have occurred in various health care settings in recent years. Because of the sensitivity of the information maintained electronically by health care organizations and facilities, breaches in these areas can be particularly damaging. Even when ALFs don't maintain medical records or information on their residents, physician groups and other entities keep such information that can be problematic for the assisted living residences if there is a breach.

Incidences Trigger Legislative Reaction

A widely publicized security breach involving a large broker of consumer health information in California brought national attention to this issue. And many people were shocked to discover that the company was not legally required to notify residents of states other than California. A flurry of legislative activity followed as states sought to protect their residents. In 2005, 27 laws were enacted in 22 states; and 70 more bills were introduced. In 2006, 25 bills were introduced in 13 states. Currently, 28 states have enacted some form of breach notification law. Most are based on California's law, which requires that any person or organization conducting business in the state report any breach of security resulting in disclosure of personal information in electronic form to an unauthorized person. The law defines "personal information" as: first name or first initial and last name and either Social Security number, driver's license number, account number, or credit or debit card number (with access code password). The law does not apply to encrypted data.

An ALF or other organization needs to understand what a security breach is before developing a policy or plan.

Not only did the widespread concern about this issue trigger legislation. It also stressed for companies and organizations that they need a sophisticated approach to privacy and security compliance because identity thieves are becoming more sophisticated. They also realized that they had much more than information to lose when security breaches occur.

What is a Security Breach?

An ALF or other organization needs to understand what a security breach is before developing a policy or plan. For example, as Hirsch noted, "Good faith use of data by employees for business purposes generally is not considered a security breach." However, if an ALF employee has a laptop computer containing residents' personal information and it is stolen from his or her car, this does constitute a potential breach.

According to California law (which is the model and gold standard for security breach legislation), companies must notify affected individuals if it "reasonably believes" that personal information has been acquired by an unauthorized person. This notification must take place "in the most expedient time possible and without unreasonable delay" and should be done in written form. Substitute forms of notice—e-mail, conspicuous posting on the entity's Web site, or notification to major statewide media—can be used only if the cost of providing notice would exceed $250,000, more than 500,000 people are affected, or insufficient contact information is available. Notification can be delayed if the organization can demonstrate that it is working actively with law enforcement to

resolve the situation. Hirsch stressed that just filing a report with the local police is not enough to rationalize delay. There must be an active, ongoing investigation.

Security Breach Planning

Even if ALFs don't store residents' medical data, it behooves them to have a plan in place to address security breaches for whatever resident-specific information they do maintain. Among the recommended elements of this plan are:

- Clear definition of what constitutes a breach
- What is considered a breach "trigger" (what event sets the plan in motion)
- How and when notification will take place (notification within 10 day sis recommended
- How telephone inquires from notice recipients will be handled
- How credit bureaus will be notified and fraud alerts handled
- Who will pay for credit checks for residents/families
- Who will coordinate interaction with law enforcement agencies

Facilities should have an incident response team in place before an actual incidence occurs. This team should involve information technology/Web management personnel, legal counsel, computer forensic experts, media relations staff, and other key facility or organizational leaders.

It is important to identify who at the facility will serve as spokesperson in case of a security breach. The ALF also must determine what this individual will say publicly and in what forum. Of course, before developing any plans or policies, it is important to know what the facility's state laws say about security breaches.

Facilities and practitioners alike should have agreements with vendors regarding private information. If possible, security breaches—what steps are being taken to prevent them, how they will be handled, and who will be responsible for associated costs—can be addressed in vendor contracts.

All of these activities take time and effort to handle. However, Hirsch emphasized that they are well worth the effort. "A response plan cannot be ad hoc," he stated.

Steps to Take After a Breach

According to Hirsch, there are five important steps to take immediately after a security breach:

- Understand your legal obligations. "Don't overact," he cautioned. He explained that jumping the gun and declaring a breach where one really doesn't exist can do more harm than good. Know the legalities surrounding incident responses, Hirsch urged his audience. "Know if your facility or company is legally required to notify residents under applicable state breach notification laws," he said, adding that notification is sometimes an ethical/corporate obligation that the organization needs to consider.
- Follow your incident response plan.
- Follow forensic procedures. "Identify internal or external forensic resources in advance," Hirsch said. "Don't wait until a situation occurs before lining up these people."
- Coordinate with law enforcement as appropriate. "Consider whether it is appropriate to contact a law enforcement agency, and choose the right one," Hirsch noted.
- Coordinate with credit reporting agencies. "Consider notifying credit reporting agencies before sending a notice to customers," Hirsch suggested. If a police report has been filed, he added, customers may find it useful to receive a copy. He also recommended that an organization consider free credit reporting for affected customers for a specific period (such as one year).

Facilities should have an incident response team in place before an actual incidence occurs.

Hirsch noted that health care facilities and organizations can avoid several mistakes that can cause problems in instances of security breaches. These errors include:

- Failure of information technology staff and lawyers to speak the same language
- Drafting a notification letter in a manner that inappropriately concedes wrongdoing
- Failure to effectively coordinate with the vendor/agent that has caused the breach
- Failure to train your workforce to spot and report a security breach immediately
- Failure to involve legal counsel at the earliest stages
- Failure to require prompt security breach notification in agreements with vendors/agents
- Lack of preparation; failure to organize the incident response team in advance so that you can respond quickly

Ready, Set, Go

Hirsch urged his audience to begin addressing these issues now. He noted that even if a facility's state doesn't have a security breach law yet, it may have one shortly. Additionally, he observed, there are several bills before Congress that would create a national law on this issue. So putting plans and policies in place now could save big headaches down the road. ALC

Bob Spence is a Maryland-based freelance writer and consultant. He is a partner in Cooper-Spence Communications.