Systematic Approach Shortest Route to Security Incident...

by David Sobel, PhD

The switchboard operator transferred the call to me on Monday morning. The woman introduced herself as "Laura Jensen" (name changed) and said that she had been seen in our ER on Saturday. She then told me that a "Dr. Sullivan" called to provide her with her lab results. After giving her the results, she said that Dr. Sullivan began asking her sexually explicit questions. She shared the questions and then said, "Look, I am angry and afraid. When I hang up I am going to call the police. I think this is coming from your ER and I want to know what you plan to do about it."

For an information security manager at a major medical center, every possible alarm was sounded by this call. A woman who was treated by our healthcare organization may have been sexually harassed by a physician or someone impersonating a physician. The police were about to get involved. And if the police got involved, the local media—television, radio, and print—would not be far behind. Nor would the threat of litigation.

In addition, members of the community who had faith in our organization would wonder about the security and confidentiality of their visits to the ER. This would be especially true for high-risk patients, such as those with HIV/AIDS or behavioral health problems. In short, this was a major information security incident and it needed our immediate attention.

As a healthcare information security consultant, I frequently ask healthcare organization senior management what happens when a major security breach occurs. How is their organization prepared to respond?

Some managers say that the risk manager handles all incidents. Others say that it depends on the type of incident. For example, if it occurs in human resources, then the director of human resources deals with the incident. Similarly, if it occurs in the laboratory, the director of laboratory medicine manages the situation. And then there are managers who answer, "We really don't have a plan." I believe that that this statement may accurately reflect the state of the affairs in many healthcare organizations.

It is naïve for senior management to assume that their organizations won't experience a serious information security incident. It is also naïve to assume that every manager will know how to handle an incident and resolve it in an effective and expeditious manner. In light of this, it would be a prudent business practice to have a group of skilled professionals respond to and manage serious breaches or incidents.

Below, we'll take a look at some ways for healthcare professionals to prepare for and manage information security breaches.

Response Team at the Ready

First, senior management should create a core incident response team (IRT). This team could be comprised of the chief operating officer, chief information officer, information security manager, HIM professional, risk manager, and legal counsel. In the event of a security incident, the team is responsible for minimizing further harm to patients and their families, reducing the possibility of adverse publicity, minimizing the possibility of litigation, and bringing the incident to a rapid conclusion.

The information security manager or privacy officer should serve as the IRT leader. All incidents should be reported to the leader, who will then decide on the severity of the issue and whether it is to be handled by a specific department or by the IRT.

Next, if the incident needs to be handled by the IRT, the leader briefs team members on the incident and obtains their counsel on how to proceed. For many incidents, this can be accomplished over the telephone. For more serious incidents, meeting face to face is recommended. Further, if the investigation is not going well, it may be necessary for the IRT to formally meet, review

all aspects of the incident, and formulate a new strategy. Communicating via e-mail is not recommended. The IRT leader should also apprise the CEO of the situation, what is being done, and who is involved in managing the incident. Once the team has been apprised, the leader contacts all parties involved in the investigative phase. Only those persons who need to be involved should be apprised of this situation; managing information security incidents is not something to be shared with a wider audience.

The IRT leader is responsible for ensuring that all conversations with aggrieved parties, as well as the steps taken by persons involved in the investigation, are carefully documented. When a case is closed, the parties most closely associated with the incident should meet to discuss what they have learned from the incident and what changes can be made to prevent a future occurrence.

Step-by-Step Resolution

A brief summary of what transpired in the days following Ms. Jensen's security complaint illustrates the above recommendations.

I explained to Ms. Jensen that our organization is committed to safeguarding patient confidentiality and that we would immediately investigate this matter. I then asked her for some specific information, such as when she was seen in the ER. I documented the entire conversation.

Next, I spoke members of our IRT and apprised them of the call and my suggestions for proceeding. I then contacted the CEO and apprised him of the call and how the team was going to proceed. I also called the director of public affairs to brief her on the matter. Finally, I called the medical staff secretary to confirm that there was no "Dr. Sullivan" on the medical staff. (Although I was correct, it didn't preclude someone on the staff from saying he or she was "Dr. Sullivan.")

Next, I met with the ER manager and assistant manager. We formulated a comprehensive plan that involved investigating when the patient came in, who was involved in her case, and who was authorized to provide follow-up information to this patient. Nursing staff looked at staff schedules and we monitored access to this patient's electronic chart to look for unusual activity.

The following day, an article appeared in the state's largest newspaper describing the complaints of seven women who were receiving obscene calls from "Dr. Sullivan." This heightened the intensity of our investigation because we were one of two major ERs in the city and the only Trauma 1 facility.

Because we were not making progress within our facility, I suggested to our legal counsel that I be permitted to contact the local police and request the names of the other women receiving the calls. In return, we would—given legal directive—release the employee to law enforcement if we found the guilty party on our staff. After weighing the potential positives and negatives, our counsel agreed that it was worth a try. I explained this to team members and informed the key people from the ER of this new tactic.

No Stone Unturned

When I spoke with the detective responsible for this case, I underscored the fact that the culprit might be on our staff and that we wanted to bring this issue to closure as quickly as possible. Later that day the detective gave me the names and ages of the six additional women. During the next several hours, we learned that only two of the women had been admitted to the ER, and that three others had outpatient laboratory work done at the medical center. The others had never been admitted to our facility. Although we were looking for any pattern that might emerge, particularly with respect to our monitoring logs, it was becoming clear that "Dr. Sullivan" did not reside within the medical center. Moreover, given the ages of these young women, I thought the calls might be coming from someone who worked for one of the major universities in the city, that is, someone who had access to students' medical records.

On the fifth day, I notified members of the IRT of my conclusions and called the detective to share my thoughts. He concurred and indicated that there was evidence pointing to one of the major colleges in town. I contacted Ms. Jensen to inform her of the results of our investigation. I also notified members of the IRT, met with ER staff and thanked them for their assistance, and documented the incident.

Two weeks later I met with members of the ER and discussed procedures around follow-up calls, new issues to add to our educational awareness program, and other matters regarding safeguarding patient confidentiality that arose as a result of this incident and investigation.

In this case, we were lucky. But no resources were spared in resolving the matter.

Every security incident should be taken seriously. Establishing and training an IRT can be a reasonable and effective way to provide a consistent and proven approach to managing these incidents. However, it is important to know when to involve local, state, and federal law enforcement. Finally, it is critical for everyone involved in managing and investigating serious information security incidents to maintain the confidentiality of these incidents and investigations both during the time of the investigation and afterwards.

David Sobel *is president of Confidentiality Matters, Inc., a firm that provides information security services to healthcare organizations and a member of the In Confidence editorial advisory board. He can be reached at dsobel@confmatters.com. For more information on Confidentiality Matters, visit www.confmatters.com.*

Article citation:
Sobel, David. "Systematic Approach Shortest Route to Security Incident Resolution." *Journal of AHIMA* 72, no.6 (2001): 64-65.
