How to React to a Security Incident

Save to myBoK

by the AHIMA 2007 Privacy and Security Practice Council

What would you do if you were notified that your organization's information system was hacked and patient information extracted? That a case manager left her laptop on the subway? That a remote transcriptionist's home was burglarized and her PC stolen? A vendor misplaced a flash drive containing patient information from your organization's laboratory logs? A home health nurse's laptop disappeared from her car?

Regardless of the sophistication of a healthcare organization's security safeguards, theft or loss of electronic personal health information (PHI) may occur. It has become a reality for many organizations in the last few years. Healthcare organizations should be prepared to respond to security incidents with a well thought-out plan.

The processes outlined on the following pages incorporate principles of HIM, quality improvement, risk management, and customer service (notification). A checklist provides guidance and necessary steps for responding to theft, loss, or unplanned destruction of electronic PHI. It incorporates investigative steps that can be taken immediately, as well as additional steps that can be taken to mitigate future incidents.

A sample security incident response form, intended for use in tandem with the checklist, can serve as the primary investigative document. Consider including all correspondence in the form by cutting and pasting key communications with identification of date and time, author, and recipients. Updating the form concurrently during the investigative process streamlines the task of organizing e-mail, notes, and other documentation. If legal counsel is involved, label the form "Privileged and Confidential Attorney-Client Communication/Work Product."

The checklist and form can be downloaded from AHIMA's FORE Library: HIM Body of Knowledge for customized adaptation and use within your organization, at www.ahima.org.

Communicating effectively and appropriately with the media is an important aspect of responding to a security incident. The sidebar [below] stresses the importance of creating communication procedures in advance.

Be Prepared to Communicate with the Media

It is in an organization's best interests to be prepared to respond to a media inquiry regarding a security incident and to have procedures in place to appropriately control the information that is shared with the public. Lack of preparation may result in a "no comment" response to the media, which may reflect negatively on the organization. It could also lead to inappropriate disclosure of information that would increase risk or harm the investigation.

Upon identification of a security incident, an organization should promptly consider its media communication plan. In an ideal situation, the organization may be able to proactively manage the media's involvement. In certain circumstances, the organization may choose to initiate contact with the news media. However, the media may be made aware of the incident and make the initial contact. Either way, the organization should have a communication procedure in place.

Designating a Communications Coordinator

Organizations should identify one individual to serve as communications coordinator. The communications coordinator can serve as the single point of contact between the organization and the media. This eliminates the need to involve members of the security incident response team and leaves them free to investigate and mitigate

the incident. However, response team members should be prepared to share information with the communications coordinator.

Organizations may take into consideration the following key points when working with the news media:

- Ensure that the communications coordinator has a clear understanding of the technical issues behind the incident so that he or she may communicate effectively and accurately with the media.
- Communicate accurate and concise information; avoid communicating misleading information, which may result in damage to the organization's reputation.
- Consult with legal counsel regarding the extent of information to be disclosed.
- Avoid communicating technical details that may entice hackers.
- Consult with investigative agencies to ensure that any details about the incident that may be used as evidence are not disclosed without approval.

Nancy Davis *(davisn@ministryhealth.org), MS, RHIA, is director of privacy at Ministry Health Care and cochair of the AHIMA 2007 Privacy and Security Practice Council.* ***Chrisann Lemery*** *(clemery@weatrust.com), MS, RHIA, of WEA Trust Insurance, is cochair of the Privacy and Security Practice Council.* ***Eve-Ellen Mandler,*** *MS, RHIA, CCS, is director of the HIM department at St. Clair Memorial Hospital.* ***Debra Mikels*** *is corporate manager, confidentiality, at Partners HealthCare System.* ***Brenda Olson,*** *RHIA, CHP, is vice president of HIM at Great Plains Health Alliance.*

Article citation:
AHIMA Privacy and Security Practice Council (2007). "How to React to a Security Incident" *Journal of AHIMA* 79, no.1 (January 2008): 66-70.