Responding to Identity Theft: One Organization's Effort to Turn a Negative Event into a Positive Result

by Jenny O'Brien, Esq.

Imagine picking up the phone and talking with a patient who informs you that he is the victim of identity theft and that he believes he was victimized while receiving treatment at your facility. It is not the type of call any organization wants to receive, but the reality is that such a call can come at any time and all organizations must be prepared to respond.

Unfortunately, this is not a hypothetical situation; it happened at a large integrated healthcare system. Upon investigating the allegation, the organization confirmed that the patient, among others, was indeed the victim of identity theft. Even more disappointing was the discovery that the theft occurred at the hand of an employee who stole Social Security numbers from medical records. The employee gave the information to others who opened fraudulent credit card and telephone accounts in patients' names.

This was a very disturbing and damaging situation that required the organization to respond to the victims, to the public's concern regarding the organization's commitment to protecting patient information, and to its employees as well. The organization needed to work hard to ensure employees were aware of their roles and responsibilities in preventing identity theft and also demonstrate that it was able to promptly and effectively respond to identity theft that occurred within one of its facilities. In doing so, it found opportunities to create positive results from a negative event.

Transparency, Engagement, and Education

The organization's responses enabled some positive outcomes from this unfortunate incident. First, thanks to the patient's phone call and a thorough investigation by the organization, the criminal behavior was stopped and the organization was able to demonstrate effective response and prevention efforts. The former employee pleaded guilty and provided assistance in the prosecution of others involved in the theft. The organization notified and worked closely with other patients who may have been affected and put credit monitoring in place to mitigate the risk and potential harm.

Once the external factors were addressed, the organization turned its focus internally. It worked with business unit leaders and representatives from operations, information services, human resources, media relations, legal, and compliance to prevent this from occurring again. The organization realized that if identity theft could happen at one of its facilities, it could happen at any facility. Accordingly, it responded to the incident with the following strategies.

Internal Risk Assessment. The organization first conducted an internal risk assessment of identify theft throughout the organization. Employees at all levels of the organization answered questions related to the organization's efforts to safeguard patient health information.

Checklist of Potential Risks. Feedback from the employee interviews led to the creation of a risk checklist. A response plan was developed for each issue raised on the checklist and communicated back to the employees, along with a plan to mitigate the identified risks.

One important realization from the assessment was that protecting against identify theft did not require unique requirements. Many of the safeguards identified in the response and prevention plan mirrored efforts already under way as part of the organization's privacy and security compliance program. For example, one employee described the threat of identity theft as a motivating factor—beyond HIPAA—in ensuring that stickers and ID bracelets containing personal health information were disposed of securely rather than thrown in a regular wastebasket.

The incident created an opportunity to engage staff in discussions around organizational strategies that could better safeguard patient information. It elevated the discussion from what the organization had to do to meet its HIPAA obligation to what the organization should do to ensure front-line employees viewed safeguarding patient information as a critical part of a patient’s episode of care.

Identity Theft Toolkit. Employees asked for more information on identity theft as well as information and resources to help them reduce both their personal risk and that of their patients. The organization developed an identity theft toolkit and posted it on the intranet as an employee resource.

Education and Training. Transparency was an important and effective strategy in the organization’s response to the incident. The organization saw the theft as an opportunity to provide additional education to staff on the importance of protecting patient information.

One effective tool was a system-wide effort to conduct brown-bag lunches using the identity theft incident to reinforce the existing HIPAA message. Employees had been receptive to ongoing HIPAA training, but when the topic of safeguarding patient information was introduced as an identity theft topic rather than a HIPAA topic, they became more engaged and sensed a stronger personal connection.

In addition, staff began taking more ownership in becoming part of the solution. One nurse described herself as a gatekeeper and more clearly recognized the key role she could play in keeping patient health information confidential.

Whether an organization is large or small, addressing real-life issues—the good, the bad, and the ugly—can be a very effective means of connecting with employees. For one organization, certainly, the negative experience of patients victimized by identity theft resulted in improving safeguards against future threat. It reinvigorated the HIPAA training program and helped the organization move beyond a mindset of privacy and security as mere compliance issues to developing organizational strategies and personal connections around safeguarding patient information.

Jenny O’Brien *(jobrien@halleland.com) is a shareholder and director of compliance services for Halleland, Lewis, Nilan & Johnson and a former compliance officer for Allina Hospitals and Clinics in Minneapolis, MN.*

Article citation:
O’Brien, Jenny. "Responding to Identity Theft: One Organization’s Effort to Turn a Negative Event into a Positive Result" *Journal of AHIMA* 79, no.4 (April 2008): 40-41.