The Healthcare Wall of Shame

Save to myBoK

While stolen laptops and hacking of healthcare computer networks have dominated the headlines, healthcare privacy and security experts warn that covered entities are ignoring the risks posed by unsecured paper records.

In response to new additions to the Office for Civil Rights' "Wall of Shame"—the informal name for the website that posts a list of breaches of unsecured protected health information affecting 500 or more individuals—OCR Deputy Director Sue McAndrew noted in a *Health Information Privacy/Alert* webinar earlier this year that theft and loss of medical records continued to be a major problem and that paper records continued to be a major source of breached records.

Harry Rhodes, MBA, RHIA, CHPS, AHIMA director of HIM practice excellence, has seen evidence of this firsthand.

"Numerous surveys of IT security administrators have revealed that of the three types of security safeguards most of the emphasis is placed on administrative safeguards, which is primarily based on policies and procedures," Rhodes says. "Far less emphasis has been placed on implementing physical and technical safeguards."

Such safeguards could be as simple as installing alarms and stronger locks on doors where records are kept, installing surveillance cameras near where records are kept, or bolting desktop computers and laptops to a desk or floor so they can't be easily swiped. With laptops, encryption of the HIPAA-protected health information would mean any theft of the device would not result in a privacy breach. But even with the technology available, many providers still refuse to utilize the encryption "get out of jail free card" in their systems, Rhodes says.

As a cautionary tale, at right is a list of the top five most egregious healthcare privacy/security breaches in the US over the last year and a half.

1. **Name of Covered Entity:** Advocate Health and Hospitals Corp./Advocate Medical Group
   State: Illinois
   Individuals affected: 4,029,530
   Date of breach: 7-15-2013
   Type of breach: Theft
   Location of breached info: Desktop computers
2. **Name of Covered Entity:** Texas Health Harris Methodist Hospital Fort Worth
   State: Texas
   Individuals affected: 277,014
   Date of breach: 5-11-2013
   Type of breach: Improper disposal
   Location of breached info: Other
3. **Name of Covered Entity:** El Centro Regional Medical Center
   State: California
   Individuals affected: 189,489
   Date of breach: 7-11-2012
   Type of breach: Improper Disposal
   Location of breached info: Paper
4. **Name of Covered Entity:** Indiana Family and Social Services Administration
   State: Indiana
   Individuals affected: 187,533
   Date of breach: 04-06-2013 to 05-21-2013

Type of breach: Other
Location of breached info: Paper

5. **Name of Covered Entity:** Crescent Health Inc.—a Walgreens Company
   State: California
   Individuals affected: 109,000
   Date of breach: 12-28-2012
   Type of breach: Theft
   Location of breached info: Desktop computer

Source: US Department of Health and Human Services. "Health Information Privacy: Breaches Affecting 500 or More Individuals." http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

Article citation:
AHIMA. "The Healthcare Wall of Shame" *Journal of AHIMA* 84, no.11 (November 2013): 88.