# HIPAA Breach Enforcement Roundup



By Victoria Cacciatore, RHIA, and Katherine Downing, MA, RHIA, CHPS, PMP

Criminal attacks on healthcare systems have risen 100 percent since 2010, according to a recent Ponemon study.[1] This makes it obvious that the privacy and security of patient health information is vulnerable and highly susceptible to data breach. The HIPAA Breach Notification Rule became effective September 23, 2013, and imposes enforcement upon those entities not in compliance. The following takes the pulse of recent breaches and security incidents within the industry, and describes the fallout that resulted from the incidents.

## Notable Health Information Privacy Breaches

As required by the ARRA-HITECH legislation, the US Department of Health and Human Services (HHS) website provides a report listing the entities involved in privacy breaches that affect more than 500 people (www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html). The spreadsheet can be downloaded and includes search options by breach type, location, covered entity type, and business associate involvement. A recent query of the report found the following notable cases:

- May 2014: HHS issued its largest HIPAA enforcement action to date, entering settlements totaling $4.8 million with two New York organizations tied to the same 2010 breach event. The event, which involved unsecured patient data on a network, affected an estimated 6,800 patients. The settlements with Columbia University and New York-Presbyterian Hospital are attributed to the organizations' lack of a risk analysis and failure to implement appropriate security policies.
- February 2014: A privacy breach at Banner Health in Phoenix, AZ, accidentally exposed personal information of more than 50,000 people in an error that resulted in their Medicare identification or Social Security numbers showing up on magazine address labels.[2] Banner Health has been working with the HHS Office for Civil Rights (OCR) on its corrective action plan, and now has policies and procedures in place that did not exist prior to the incident.
- April 2014: University Urology, PC of Knoxville, TN, informed patients of a data breach that included names and addresses but no Social Security numbers. According to a statement by the facility, an administrative assistant had compiled the data in an effort to sell it to a competing provider, helping them gain patient business. Patients contacted University Urology to let them know that the competing provider had been soliciting their business.
- December 2013: St. Joseph Health System, based in Bryan, TX, had a data security attack originating in China and other countries in which certain parties gained unauthorized access to a single server containing patient and employee files. This breach exposed 405,000 patients, employees, and beneficiary Social Security numbers.

## Notable Health Information Security Breaches

Security breaches can happen internally, externally, virtually with an electronic health record (EHR) system, or physically with theft of equipment. On February 5, 2014, Sutherland Healthcare Solutions experienced a medical data security breach that contained the information of 338,700 individuals. Sutherland Healthcare Solutions is a business associate of the County of Los Angeles and handles the medical billing and collections for the Department of Public Health. Individuals stole eight computers and two monitors from the provider. The computers contained data including patients' first and last names, Social Security numbers, certain medical and billing information, and possibly birth dates, addresses, and diagnoses.[3] It is unclear whether or not the thieves knew about the sensitivity of the information stored in the computers. The burglary is currently under investigation.

Kaiser Permanente's Northern California Division of Research detected a breach when it discovered that a server infected with malicious software caused a breakdown in the server's security barriers, allowing the hackers to obtain personal information. The information included first and last names, dates of birth, age, gender, address, race and ethnicity, medical record numbers, and lab results—all associated with research provided by individuals as part of various research studies.

Tracy Lieu, MD, the division's director, explained in a statement to the media that state and federal authorities had been notified and "we are continuing to take appropriate steps to help prevent future incidents like this."

The second largest breach ever reported occurred at Advocate Medical Group in Illinois. This breach included the theft of four laptops containing the sensitive information of more than four million patients. HIPAA fines and penalties have not yet been settled in the case, nor has the corrective action plan been enacted as of press time. Patients affected have, however, filed a $4.9 billion class action lawsuit.[4] This is only the beginning of the penalties that will be assessed due to Advocate's data breach. Not only will Advocate be penalized and sued, they risk losing the respect of the community and their trusted name.

The average cost to an organization or provider per lost or stolen record is $188, according to data from OCR.[5] However, penalties will vary and can be costly, usually based on the extent of harm they can potentially have on affected individuals. Find information about HIPAA penalties, case examples, and resolutions at www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

## Defining and Preventing Breaches

The privacy and security of patient information is a key component of an organization's integrity. In order to prevent a breach, an organization must clearly understand what constitutes a breach. The breach notification rule defines a breach as:

> An impermissible use or disclosure under the (HIPAA) Privacy Rule that compromises the security or privacy of the protected health information (PHI). An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
>
> 1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification
> 2. The unauthorized person who used the protected health information or to whom the disclosure was made
> 3. Whether the protected health information was actually acquired or viewed
> 4. The extent to which the risk to the protected health information has been mitigated.[6]

If a breach of unsecured PHI has occurred, it is the duty of the covered entity or business associate to notify the individuals involved, the HHS Secretary, and the media if more than 500 individuals were affected. Refer to AHIMA's "Breach Management Toolkit" for further details and information for managing breaches.

## New HHS Security Risk Analysis Tool Available

While staying current on HIPAA breach enforcement is integral to the security of patient information, it is not always possible to prevent a breach. As an organization, it is necessary to perform a risk analysis to improve the privacy and security of patient information. A new security risk assessment (SRA) tool has been released by HHS that can be used to verify one's assessment process or complement it. The tool is available at www.healthit.gov/providers-professionals/security-risk-assessment.

Other key areas of focus for reducing the risk of a breach are educating employees on privacy and security policies, passwords, and encryption. The hefty fines, indiscretion, and time needed to repair a breach not only hurt the covered entities' finances, but hurt their brand as well.

## Notes

1. Ponemon Institute. "Fourth Annual Benchmark Study on Patient Privacy and Data Security." March 2014. http://www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security.
2. Landen, Rachel. "Banner Health data breach affects more than 50,000." Modern Healthcare. February 2014. http://www.modernhealthcare.com/article/20140226/NEWS/302269946.
3. Sewell, Abby. "Computers with L.A. County patients' personal data are stolen." Los Angeles Times. March 6, 2014. http://articles.latimes.com/2014/mar/06/local/la-me-patient-data-stolen-20140307.

4. Vogel, David. “Top 10 HIPAA Data Breaches of 2013.” Layered Tech Official Blog. http://www.layeredtech.com/blog/top-10hipaa-data-breaches-of-2013/.
5. Department of Health and Human Services. “Breach Notification Rule.” http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.
6. Ibid.

Katherine Downing (Kathy.Downing@ahima.org) is a director of HIM practice excellence at AHIMA. Victoria Cacciatore (vickycacc@live.com) is a recent graduate from the University of Illinois at Chicago and a former AHIMA intern.

**Article citation**:
Cacciatore, Victoria; Downing, Katherine. "HIPAA Breach Enforcement Roundup" *Journal of AHIMA* 85, no.7 (July 2014): 42-43.