PRIVACY PROFESSOR

HIPAA felony convictions, sanctions and upcoming trends

By Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

February 24, 2009

Scant Compliance Activity During Decade Of HIPAA

On August 21, 1996, the U.S. Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA Privacy Rule went into effect in April 2001, and gave covered entities (CEs) two years to meet compliance. The HIPAA Security Rule went into effect in April 2003 and CEs had until April 2005 to get into compliance. As of August 24, 2007, the Centers for Medicare & Medicaid Services (CMS), responsible for the HIPAA Security Rule enforcement, and the Office for Civil Rights (OCR), responsible for HIPAA Privacy Rule compliance, had not even established any policies or procedures for conducting compliance reviews at CEs[1]. This even though a significant number of HIPAA complaints had been received.

NOTE: Through the end of December, 2008 the OCR had received 41,807 HIPAA complaints[2], with 6,019 (14%) of the total still open. As of January 31, 2009, CMS had received 1,044 complaints and still had 149 (14%) of the total still open.

The U.S. Department of Health and Human Services (HHS) never performed a compliance audit until March of 2007 when Atlanta's Piedmont Hospital was the first to feel the scrutiny of HHS Office of Inspector General's (OIG) auditors looking at HIPAA Security Rule compliance. The impact of that specific audit was underwhelming in that a summary of the findings have not yet been published. However, the audit caught the attention of many CEs who had long ago assumed that since no compliance enforcement actions had occurred since 2003, that there would never be any such actions. The tide appeared to be ebbing.

In October 2007, the CMS contracted Pricewaterhouse Coopers to do up to twenty HIPAA Security Rule compliance audits in the next few months. This was in addition to the audits being performed by the HHS OIG according to Tony Trenkle, the director of the CMS Office of E-Health Standards and Services[3]. The compliance enforcement tide was turning.

Growing HIPAA Criminal Activity

Despite the huge number of complaints, as of February 25, 2009 there have been only two non-compliance sanctions applied by the HHS, compared to eight HIPAA criminal felony convictions, as listed in Table 1.

Table 1

HIPAA criminal convictions		
Date	Situation	Penalty
December 2008	Andrea Smith, from Trumann, Arkansas, convicted of accessing and disclosing a patient's health information from her place of employment for personal gain.	Sentenced to two years probation and 100 hours of community service

[1] Retrieved on 02/24/2009 from http://www.oig.hhs.gov/oas/reports/region4/40705064.pdf
[2] Retrieved on 02/24/2009 from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/numbersglance013109.html
[3] Retrieved on 02/21/2009 from http://www.aishealth.com/Compliance/Hipaa/RPP_CMS_HIPAA_Security_Reviews.html

May 2008	Leslie A. Howell, who worked at an Oklahoma City counseling center gave patient files to Ryan Jay Meckenstock and Nicole Lanae Stevenson who used the files "to make counterfeit identification papers that helped them obtain merchandise and credit from a number of retailers."	Sentenced to 14 months in prison.
February 2008	Ryan Jay Meckenstock and Nicole Lanae Stevenson used stolen patient files from Howell, as well as from stolen/discarded mail, internet searches, credit reports, and car burglaries, to produce counterfeit identification documents (IDs) to obtain merchandise and credit from various merchants.	Meckenstock was sentenced to serve 119 months in federal prison. Stevenson was sentenced to serve 168 months in federal prison. Each defendant was ordered to pay $101,896.39 in restitution to their victims.
January 2007	Isis Machado, an employee at the Cleveland Clinic in Weston, Florida, was charged with obtaining computerized patient files, downloading individually identifiable health information of over 1,100 Medicare patients, and then selling the information to her cousin, Fernando Ferrer, Jr., the owner of Advanced Medical Claims in Naples, Florida. Ferrer then used the information to submit approximately $2.8 million in fraudulent Medicare claims.	Machado and Ferrer were each found guilty of conspiring to defraud the United States, one count of computer fraud, one count of wrongful disclosure of individually identifiable health information. Ferrer was sentenced to 87 months in prison to be followed by three years of supervised release, and must pay $2.5 million in restitution. Machado was sentenced to three years probation, including six months of home confinement, and ordered to pay $2.5 million in restitution.
March 2006	Liz Arlene Ramirez was convicted for selling the individually identifiable health information an FBI agent to a drug trafficker and in exchange for $500.	Sentenced to serve six months in jail followed by four months of home confinement with a subsequent two-year term of supervised release and a $100 special assessment.
August 2004	Richard Gibson, who was an employee of the Seattle Cancer Care Alliance, a treatment center for cancer patients, stole patient information and used it to obtain credit cards in that patient's name, then used them to receive cash advances and to purchase various items, including video games, home improvement supplies, apparel, jewelry and gasoline valued at $9,139.42.	Signed a plea agreement, and was convicted and sentenced to sixteen months in prison. As part of his plea bargain, Gibson agreed to make restitution to the credit card companies whose cards he had used to make illegal purchases and to the victim of his identity theft.

HIPAA non-compliance sanctions			
Date	Company	Situation	Penalty
02/18/09	CVS pharmacies	Disposal of PHI	$2.25 million + information security improvements + ongoing audits
07//08	Providence Health & Services	Loss of electronic backup media and laptop computers	$100,000 + implement a detailed Corrective Action Plan to ensure that it will appropriately safeguard

		containing individually identifiable health information	identifiable electronic patient information against theft or loss

All eight of the criminal convictions were basically the result of insiders, with access to protected health information (PHI) abusing that authorized access to commit crimes. The insider threat has always been significant. It is likely to become even more of a concern.

Desperate Times Increase The Crimes

It is not uncommon for healthcare entities to be favorite targets for crime. If you look through the annals of the growing number of sites that chronicle privacy breaches, such as the Privacy Rights Clearinghouse (PRC) Chronology of Data Breaches (http://www.privacyrights.org/ar/ChronDataBreaches.htm) and the Open Security Foundation's DataLossDB (http://datalossdb.org), you will see an overwhelming number of incidents from healthcare providers and healthcare insurers. In December 2008 alone there were seven healthcare breaches listed in the PRC listing that involved 13,000 health records. Keep in mind there are significant numbers of other breaches that are not listed in any of these compendiums, let alone even reported in the news.

When the economy was good there were plenty of instances of criminals and insiders taking PHI, and other types of personally identifiable information (PII) to do bad things. The bad economy now provides even greater motivation for people to do even more bad things.

Poor information security practices within CEs provide great opportunity for crime to occur. A significant portion of personnel, business partners and others with authorized access to medical information will succumb to temptation to do bad things for financial gain if they think they won't get caught, if they feel their job is threatened, or if they believe their employer is mistreating them. Criminals with no authorized access will exploit security weaknesses to obtain patient information and use it for their financial gain.

Healthcare organizations posses a huge amount of very valuable PII, such as credit card numbers, insurance policy numbers, Social Security numbers, banking information, along with names, addresses, phone numbers and other information that can easily be used for identity theft. Increasingly some of the most valuable information is that for patients with preferred medical network insurance plans. Criminals can take this information and sell to other criminals who can then use it in their illegal immigration activities. PHI is also progressively being used more for medical identity theft for individuals desperate to obtain healthcare insurance coverage, but who otherwise do not qualify for it.

Insider Threat Is Increasing

There have been numerous reports about the growing instances of insiders (individuals with authorized access to information) stealing information. Numerous news reports have indicated that as organizations cut costs, insider threats are rising, and cybercriminals are using the resulting lax security to do even more cybercrime. According to a recent report[4]:

- 56% of workers surveyed admitted to being worried about losing their jobs.
- Over half have already downloaded competitive corporate data and plan to use the information as a negotiating tool to secure their next job
- 58% of US workers have already downloaded business data, including customer PII, to take with them if they lose their jobs.

Just a few examples of insider crime cases within healthcare organizations include:

[4] "The Global Recession and its Effect on Work Ethics"; retrieved 02/24/09 from http://www.cyber-ark.com/news-events/pr_20081201.asp

- On January 16, 2009, Remberto Sarmiento was sentenced to eight years in prison for submitting over $7,000,000 in fraudulent claims to the Medicare program for reimbursement by using stolen patient information. Remberto purchased two medical companies, maintained corresponding corporate bank accounts, signed checks drawn on those bank accounts, and then distributed fraud proceeds using a shell construction company.
- In January 2008, Tenet Healthcare Corporation, which owns more than 50 hospitals in a dozen states, disclosed a security breach involving a former billing center employee in Texas who pled guilty to stealing patient information on as many as 37,000 individuals. He got nine months in jail.
- In January, 2008, an office cleaner at the HealthSouth Ridgelake Hospital in Sarasota, Florida pled guilty to taking information from the patient files of an anesthesiologist and then committing fraud by ordering credit cards on the Internet with stolen patient information. He got two years jail time.

Personnel may also purposely sabotage computer systems if they feel their employment is threatened. For example, on August 27, 2007 a federal jury found Jon P. Oson, a former computer network engineer and technical services manager for the Council of Community Health Clinics, guilty of two counts of violating the Computer Fraud and Abuse Act. After he got a bad performance review, in retaliation Oson disabled the systems backups of patient information and also deleted patient data on many of the servers. Not only did Oson do damage to the clinics' business systems, but Oson's actions could very well have negatively impacted the medical care of the people whose PHI he deleted.

Here are just a few of the important steps healthcare organizations should take to fight the insider threat, in addition to supporting HIPAA compliance:

1. Make sure one person does not have all authority, control over, or access to critical and sensitive data. This is a situation that can be hard to address within small and medium sized businesses (SMBs), but it is something important to do if possible.
2. Make sure multiple generations of backups are made of critical systems and data, and ensure copies are stored in a secure offsite location. You don't want malicious former employees able to get to the backups and erase them.
3. Log the access of personnel with authorized access to sensitive data and systems. When management knew there was going to be a negative performance review given to Oson, others outside Oson's line of management should have started logging Oson's access to the systems for which he was responsible, if it wasn't being logged already. No one individual should be controlling the entire network and data resources. If this is the situation, there should be another position, outside the individual's area, logging and monitoring the individual's activities.
4. Have thorough exit plans in place and follow them consistently for when employees in critical positions are terminated or resign. As soon as Oson resigned, all his access, especially including from remote locations, should have been immediately terminated. There should also be heightened monitoring following the unharmonious resignation of an employee from a position of excessive systems and data access control and responsibility.

HIPAA Crime And Compliance Enforcement Trends

There is growing demand for more accountability and penalties for HIPAA non-compliance as well as for data breaches including PHI. CEs are starting to take notice, and take action. In the coming months expect to see a trend for more criminal prosecutions and compliance enforcement activities.

More covered entities are strictly enforcing their policies

In the past year there have been numerous reports about HIPAA CEs applying their own organizational sanctions against personnel who violate their information security and privacy

policies that are also violations of the HIPAA requirements. This is good; policies are not effective if they are not enforced and sanctions consistently applied!
For example, consider the Catskill Regional Medical Center in Harris, New York, which apparently takes the HIPAA requirements seriously and put controls in place to catch employees who are looking through patient files when they have no job need to do so.

In February 2009 an employee was fired for looking through 431 files of patients who she knew or worked with. Some good security practices were likely in place to be able to catch this employee:

- The employee was caught as a result of an audit. This means that there were access logs of some type(s) in place to document whenever someone accessed patient files. Does your organization log whenever someone accesses the PII within your enterprise?
- The snooped-upon patients were notified. This is not only a good breach response practice, it is also required by at least 46 U.S. breach notice laws.
- The hospital actively enforced the sanctions for non-compliance with their own internal policies as well as with federal laws. Does your organization consistently enforce sanctions for policy and law non-compliance?
- The hospital likely had ongoing awareness communications and regular training in place to be able to fire the employee. Do you have effective training in place?

This is also a good example of the insider threat. In this case, it was reported that the motivation for the person to snoop was merely curiosity; she had access so she took advantage of that access even though she had no business need to look at the records. Do you wonder how many of the physical, hard copy records she snooped through, too? It's harder to log access to papers as opposed to digital files.

More HIPAA HHS audits, and more resulting sanctions for non-compliance
There is also much more push from the government to more actively enforce HIPAA to help reduce PHI breaches. This was made crystal clear on February 18, 2009, when, as part of the U.S. stimulus package, President Obama signed into law the Health Information Technology for Economic and Clinical Health Act HITECH Act), which significantly expands the reach of the HIPAA Privacy Rule and Security Rule, along with the corresponding penalties.

One significant resulting change is that HIPAA will now basically apply to CE business associates (BAs) directly. BAs were already required to follow the security that the CEs put into their contracts. I've done over 150 BA security program reviews, which included review of the contracts, and the security requirement details within these contracts typically have been missing at worst and vague and incomplete at best. Add to this that the risk to the BA for non-compliance was basically just for a contractual breach for failure to comply, and you are left with little motivation for the BAs to invest the time, personnel and resources necessary for effective safeguards. This has now changed. The HITECH Act includes a statutory obligation for BAs to comply with HIPAA, and BAs now face noncompliance enforcement actions from the HHS, in addition to also possibly receiving civil and criminal penalties for noncompliance and for PHI breaches occurring from compliance failures.

The HITECH Act also increases the penalties for HIPAA violations of HIPAA. The HITECH Act authorizes State Attorneys General to bring civil action in Federal district court against individuals who violate HIPAA. The original HIPAA rules authorized the HHS Secretary to conduct compliance reviews but do not have specific requirements. The HITECH Act now requires ongoing audits to ensure Privacy Rule and Security Rule compliance.

Another important change that HITECH Act brings to HIPAA is PHI breach notification, which was not part of the original HIPAA rules. This is significant to CEs and BAs, even though there are at least 46 state level breach notice laws. To date few CEs had privacy breach response and notice plans in place.

More HIPAA criminal prosecutions and convictions
As Table 1 shows, more criminal convictions are starting to occur. What the table does not show is that there are many more active prosecutions of HIPAA criminal activities that have not yet been resolved. In April 2008, a Department of Justice (DOJ) spokesperson reported that the department has filed over 200 criminal cases since 2003 under a statute that includes HIPAA, but that not all cases are necessarily HIPAA-related.[5]

Originally HIPAA provided for criminal penalties of fines of up to $250,000 and up to 10 years in prison for disclosing or obtaining PHI with the intent to sell, transfer or use PHI for commercial advantage, personal gain, or malicious harm. In July 2005, the Justice Department ruled that only a CE could be criminally liable and prosecuted under HIPAA. The HITECH Act has changed this by allowing criminal penalties for wrongful disclosure of PHI to apply to individuals who obtain or disclose PHI maintained by a CE, whether or not the individuals themselves are employees of a CE.

The HITECH Act also permits the OCR to pursue an investigation and apply civil monetary penalties against individuals for criminal violations of the HIPAA Privacy Rule and Security Rule if the Justice Department did not prosecute the individuals. Additionally, the HITECH Act changes HIPAA to require formal investigations of complaints and to impose civil monetary penalties for violations resulting from willful neglect. Any civil monetary penalties collected must then be transferred to OCR to use for HIPAA enforcement activities, and the HHS must establish a process to distribute a percentage of the collected HIPAA penalties to harmed individuals.

[5] Rubenstein, Wall Street Journal, 4/29/2008