ABC's HIPAA News!

Fall, 2004

Feds Successful With First HIPAA Privacy Conviction!...*We Think!* What Does this Mean to Covered Entities?

By: Dorothy M. Cociu
President, Advanced Benefit Consulting & Insurance Services, Inc.

Well, it's happened! The first federal conviction for a HIPAA Privacy violation! *HIPAA Privacy is real!* And the conviction happened sooner than the industry may have guessed… But then again, it was based on a plea agreement, and not a lengthy trial, which may have sped up the process immensely. And another very important "but"…..*it's not quite final.*

On August 19, 2004, Richard Gibson, a Seattle, Washington-based former employee of the Seattle Cancer Care Alliance, pleaded guilty to violating the HIPAA Privacy Rule. This was the first criminal conviction, which resulted from a plea bargain, under the Privacy Rules of the Health Insurance Portability and Accountability Act, which was effective as early as April 14, 2003. This "conviction" is expected to be accepted by the presiding judge, but the real "success" of the case won't be known until November. The case was investigated by the FBI.

Mr. Gibson admitted to using a patient's name, date of birth, and social security number, obtained during his employment with the Cancer Care Alliance, for personal gain, resulting in the illegal request and receipt of credit cards between October, 2003 and January, 2004. Once in possession of the credit cards, Mr. Gibson charged more than $9,100 on the credit cards for video games, clothing, home improvement supplies, jewelry, gasoline, groceries and other items, according to federal prosecutors.

Under the plea agreement, Gibson pled guilty to one count of wrongful disclosure of individually identifiable health information. He agreed to accept a sentence of 10 to 16 months, plus restitution to the credit card companies and patient. The case will be reviewed by U.S. District Court Judge Richard Martinez on November 5th. Judge Martinez will, following his review of the plea agreement, either accept the sentence or impose his own. If the Judge rejects the plea agreement, Mr. Gibson will have the opportunity to withdraw his guilty plea.

U.S. Attorney John McKay stated "This case should serve as a reminder that misuse of patient information may result in criminal prosecution."

Under the HIPAA Privacy Rule, criminal use of patient information for personal gain is punishable by imprisonment for up to ten years, and a fine of up to $250,000. Those are, of course, maximums. Was the plea agreement here too lenient? That's hard to say, as this was the first conviction, and we are dealing with a plea agreement in a criminal matter. It is likely that other charges were filed, and some sort of deal was made, allowing the defendant to plead guilty

to a lesser charge. A lesser penalty may have saved taxpayer dollars on prosecuting a lengthy case, and spending months or years on a federal criminal trial. I asked Sheldon Emmer, attorney from Emmer & Graeber, an employee benefits law firm in Los Angeles, his thoughts on the case and the plea agreement. "You don't use the prosecutorial resources to go through a long trial, and you're not taking up court time with trials, so you always need to take a plea agreement with a grain of salt. This is not yet a sentence. This is just a proposal by the U.S. Attorney that Gibson has agreed to. The judge has to approve it. In addition to the 10-16 months, he has to pay restitution of almost $10,000 plus the patients' costs incurred, if any, plus the $100 fee for the plea agreement. The theory of any criminal sentencing is that it is supposed to be proportional to the crime. Here, when it's the first conviction, it's hard to put into context. The analogy is sort of like the subjective judging at the Olympics in gymnastics. The early performers may not get as high a score as if they'd done the exact same performance later in the competition. The judges want to keep room above that to give someone a higher score if they've done a better performance later on. It's sort of like here, if next time there is a Zone C conviction, they want to be sure it is about the same in terms of culpability, and the level of crime the next person has committed should be proportional to this one. You don't want to give this person 50 years, and then what do you do with someone who does it twice as bad? Obviously you can't go over ten years anyway [in HIPAA Privacy matters], as that is the maximum. What, in our wildest dreams, could we imagine would be *so bad* that it deserves the maximum, and then we scale it back from there."

So, how does the system judge this first HIPAA Privacy violation? I guess we will find out soon enough; after November 5th. Mr. Gibson was, incidentally, fired by the Seattle Cancer Care Alliance after the identity theft was discovered.

A question remains, however….Isn't this case more credit card fraud, identity theft, and a combination of other criminal areas, more so than a HIPAA Privacy violation? "We don't have all the facts in the plea agreement," commented Mr. Emmer. "We know that there were other charges. This is probably the easiest of the charges to prove; maybe the defense attorney negotiated a deal because this was the lightest sentence. The FBI was investigating it. Technically it was HIPAA Privacy theft, of protected health information, because he received it in the context of where he worked, in the context of patient information. It's the first case, but I think this is more a matter of whether the federal government is serious about it, *but this was a negotiated deal*."

What does this conviction mean to Covered Entities? Will there be an impact on providers, insurers, employers sponsoring health plans, or other covered entities? My guess is, that for those who are conscientious, there will be tighter screening of employees, particularly any employees with access to PHI, stronger firewalls and better overall security. Proper employee training is also key. But then again, there are always those who think they simply don't need to comply, so we'll see if this changes things in any way.

As a reminder, covered entities have many requirements under HIPAA Privacy. They must appoint a Privacy Officer and receive training. They must also train employees according to their job functions. Additionally, certain requirements, such as an Action Plan, policies and procedures on privacy, and a number of other tasks are required. To detail the necessary requirements goes far beyond the scope of this article.

What have we learned from this first case? Where do we stand with enforcement? Other than this first case, have there been other enforcement activities? According to comments made by Susan McAndrew, Senior Advisor for HIPAA Privacy Policy at HHS' Office for Civil Rights (OCR) in the Employer's Guide to HIPAA Privacy Requirements, August, 2004, Thompson Publishing, OCR generated a database of the first year's complaints from April, 2003 to April, 2004 for the Federal Government Accountability Office, which is preparing a report on HIPAA Privacy Implementation. The agency, according to the article in Thompson's guide, *received more than 6,500 total complaints by May 31, 2004, and was getting between 120 and 130 new ones per week,* noted McAndrew.

"Privacy continues to be in the forefront of everyone's agenda," McAndrew said. "Consumers are becoming aware of their rights and exercising their rights, and are very protective of concerns that their privacy rights may be breached by covered entities."

OCR, according to the Thompson guide, has not yet sought civil monetary penalties in any of these cases but has referred about 80 possible criminal violations to the U.S. Department of Justice, which is "continuing to investigate and pursue those cases that they think have merit," McAndrew said.

"I think what this shows us is that maybe the government is really serious in its enforcement," stated Emmer, "but theoretically these entities were supposed to have been complying since April 14, 2003. I think that they [covered entities] should have been taking steps all along. People that don't think they'll get caught still don't think they'll get caught. We need to

remember that one of the concerns that Congress had when passing HIPAA privacy was concern with identity theft, and this is what we have here. It remains to be seen whether this law is going to be rigorously enforced or not."

I, however, think that if OCR has received such a high level of complaints, and they have gone on record as recently as August with Thompson as to how serious this is, that the enforcement efforts will continue to be a high priority. Now that there has been a prosecution, I think this will escalate as far as importance. I also believe that as the public becomes more educated, the number of complaints will also escalate – most likely far beyond the 120 to 130 per week received as of the first year. Remember, as of the first year, only large plans, above $5 million in receipts, needed to be compliant. A lot more plans had an effective date of April 14, 2004. So, I would not be surprised if HHS/OCR HIPAA Privacy audits are just around the corner. Generally, from my experience and observation, audits don't start until at least one year after the compliance date. Now, we have one year under our belts for large plans, with a compliance date of April 14, 2003, so audits don't seem that far-fetched. And if OCR thinks this is a high priority, it would be wise to think they will continue their enforcement efforts. They have not yet sought civil penalties, as it looks like they were focusing first on criminal actions. So, again, logic suggests to me that civil penalties are next…and with over 6,500 complaints in the first year, there are a lot of enforcement (i.e. audit) possibilities out there.

Now let's imagine your (our) world…..Imagine the employer who sponsors a health plan, who doesn't properly protect PHI. Someone at the firm gets his hands on that highly valuable piece of private information…he later uses it to harm the participant and/or for financial or other personal gain. A federal criminal investigation follows by the FBI….The employee/participant of course files a privacy complaint, so now the Department of Health and Human Services (HHS) is also involved, and/or the Office of Civil Rights. An audit is scheduled, to review the employer's privacy policies, and civil penalties may be handed to the employer….Many hours of productivity are lost by the employer….The employee/plan participant is now disgruntled. Lots of panic takes place. Who is responsible? What is the true cost of noncompliance? *Only time will tell….##*

Notes: For a copy of the Plea Agreement, or related news and information, please visit our website at www.advancedbenefitconsulting.com. Special thanks to Sheldon Emmer, Attorney and President of Emmer & Graeber, A Law Corporation, in West Los Angeles. Mr. Emmer can be reached at (310) 475-3792. For products or services to assist in HIPAA Compliance, please visit our website or call us toll free at (866) 658-3835.

Ms. Cociu is the author of The ABC's of HIPAA Compliance – An Employer's Simplified Guide to HIPAA Compliance. This manual, plus training videos, posters, and live seminar training is available from Advanced Benefit Consulting.

ABC's HIPAA News is published by Advanced Benefit Consulting & Insurance Services, Inc. P.O. Box 1941, Big Bear Lake, CA 92315-1941. (909) 878-9210, or toll free (866) 658-3835. Fax (909) 878-9211.

Reference Sources: Plea Agreement, United States District Court Western District of Washington, at Seattle, CR 04-0374 RSM; Employer's Guide to HIPAA Privacy Requirements, Thompson Publishing, August, 2004, Employee Benefit Series, Volume 3, No. 7.