



Client Alert

Contact Attorneys Regarding
This Matter:

Aaron M. Danzig
404.873.8504 - direct
404.873.8505 - fax
aaron.danzig@agg.com

Sidney S. Welch
404.873.8182 - direct
404.873.8183 - fax
sidney.welch@agg.com

Arnall Golden Gregory LLP
Attorneys at Law
171 17th Street NW
Suite 2100
Atlanta, GA 30363-1031
404.873.8500
www.agg.com

Sneak Peek Leads to Guilty Plea – A Cautionary HIPAA Tale

On January 8, 2010, a researcher with the UCLA School of Medicine became one of just a handful of people in the United States to be convicted of violating the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA). In pleading guilty to four separate misdemeanor counts of violating HIPAA, he admitted to obtaining individually identifiable health information without a valid reason, medical or otherwise. The defendant was a licensed cardiothoracic surgeon in China, working at UCLA as a researcher. In October 2003, he was given notice that he would be terminated. After that and while still employed, he accessed his supervisor's and other coworkers' medical records. He then continued to access the medical records of other patients, including well-recognized celebrities. All totaled, he illegally accessed the UCLA patient records system more than 300 times in a three-week period.

After the guilty plea, the acting U.S. Attorney in Los Angeles stated, "HIPAA's criminal privacy provisions protect not only celebrities, but all of us from curious neighbors, disgruntled coworkers and other snoopers." The defendant is to be sentenced on March 22, 2010. He could face up to four years in prison, one year for each misdemeanor, although it is more likely that, if he receives a term of imprisonment for his crimes, it would be one year or less.

This occurrence is not the first time an employee at UCLA has been charged with illegally accessing patient records. In 2008, another employee accessed celebrity records and sold them to the *National Enquirer*. The employee was charged and pleaded guilty but passed away from cancer prior to sentencing, so her case was dismissed. Most of the other HIPAA-related prosecutions over the past few years, including prosecutions in Seattle, Washington, and Florida, related to situations where the defendants accessed and stole protected health information (PHI) for personal gain, such as using the stolen information to obtain credit cards. However, prosecutions have also occurred, similar to the UCLA case, where someone accesses PHI just out of curiosity. For example, in July 2009, three employees of an Arkansas hospital pleaded guilty to misdemeanor HIPAA violations for illegally accessing medical records of a local television personality who had been brutally beaten in her home and passed away at the hospital. The three individuals were fined and placed on one year's probation.

HIPAA was passed in 1996 and promulgated to reduce costs by standardizing the processing of healthcare transactions, in addition to improving the

portability of health coverage, increasing the security and privacy of healthcare information and making other changes to the healthcare delivery system. While HIPAA has many different provisions, at issue in the criminal cases described above are the privacy and security standards, which were designed to protect the confidentiality, integrity and availability of people's healthcare information. Under HIPAA, Covered Entities, which include a health plan, healthcare clearinghouse, or Healthcare Provider, may not use or disclose PHI, except as specifically allowed in the statute and regulations or as the individual, who is the subject of the information (or the individual's personal representative), authorizes in writing in advance of the release of the information.

HIPAA provides for civil and criminal penalties for violating its standards and requirements. Since the passage of the HITECH Act, which modified HIPAA regulations and was included in the so-called "Stimulus Act of 2009," the civil monetary penalty (CMP) provisions of HIPAA are amended and now include tiered increases ranging from \$100 to \$50,000 for each violation. The minimum fine can be up to \$10,000 if the person's or company's actions were deemed to willfully neglect HIPAA regulations.

The criminal penalties that HIPAA imposes can be severe for certain violations. A person who knowingly, and in violation of the HIPAA privacy rules, discloses PHI to another individual faces a range of possible penalties depending on the facts. The base set of penalties includes a fine of not more than \$50,000 and imprisonment of not more than one year, or both. These penalties would be a misdemeanor, as the maximum term of imprisonment is under one year. However, HIPAA also provides for felony charges. If the offense is committed under false pretenses, the person may be fined not more than \$100,000 and imprisoned for not more than five years, or both. If the offense is committed with the intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm, the person may be fined not more than \$250,000 and imprisoned for not more than 10 years, or both.

The possibility of a criminal conviction for taking a sneak peek at a patient's medical records may be something that health care practitioners and office staff would never consider. Acting on a curious impulse, however, may result in a severe penalty. The UCLA case, and other HIPAA-related prosecutions, should serve as cautionary warnings to any healthcare employee and strong reminders to be aware of, and comply with, all HIPAA rules and regulations. The failure to do so may have troubling and lasting implications.

Arnall Golden Gregory LLP serves the business needs of growing public and private companies, helping clients turn legal challenges into business opportunities. We don't just tell you if something is possible, we show you how to make it happen. Please visit our website for more information, www.agg.com.

This alert provides a general summary of recent legal developments. It is not intended to be, and should not be relied upon as, legal advice.