HIPAA Criminal Prosecutions: Few and Far Between

Doreen Z. McQuarrie, J.D., L.L.M. candidate

Although the criminal enforcement provisions to the 1996 Health Insurance Portability and Accountability Act ("HIPAA")[1] went into effect nearly four years ago and set the stage for criminal prosecutions against violators, there have been only four criminal HIPAA violations prosecuted in the United States to date. During that four year period over 350 complaints were considered by the Department of Justice (DOJ),[2] which is responsible for enforcement of the HIPAA criminal provisions.[3] That the DOJ has prosecuted only four cases raises questions regarding the effectiveness of the enforcement provisions and the priority the DOJ has assigned to prosecution of HIPAA violations.

It is unclear exactly how many complaints have been filed with the DOJ. However, according to Melamedia's HIPAA Statistics Update Service,[4] the Office of Civil Rights (which is charged with investigating complaints and civil enforcement of HIPAA's privacy regulations)[5] has referred a total of 366 complaints to the DOJ for further investigation of potential criminal violations.[6] The elements of a criminal offense under HIPAA are fairly straight forward. To whom the provisions apply, however, has been and continues to be the subject of debate and quite possibly could be an explanation for why criminal violators are escaping punishment.

To commit a "criminal offense" under HIPAA, a *person* must knowingly and in violation of the HIPAA rules do one (or more) of the following three things: use or cause to be used a unique health identifier, obtain individually identifiable health information relating to an individual, or disclose individually identifiable health information to another person.[7] Criminal penalties under HIPAA, tiered in accordance with the seriousness of the offense, range from a fine of up to $50,000 and/or imprisonment for up to a year for a simple violation to a fine up to $100,000 and/or imprisonment up to five years for an offense committed under false pretenses and a fine of up to $250,000 and/or imprisonment up to ten years for an offense committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.[8] Three of the four cases prosecuted to date involved the theft of

---

[1] 42 U.S.C. § 1302d-6 (2000).
[2] *See* discussion *infra.*
[3] *See* Fact Sheet, United States Department of Health & Human Services, Protecting the Privacy of Patients' Health Information (Apr. 14, 2003), *available at* http://dhhs.gov/news/facts/privacy.html.
[4] HIPAA Enforcement Statistics Update Service E-mail from Dennis Melamed, President of Melamedia L.L.C. to author (Feb. 13, 2007).
[5] *See* Fact Sheet, *supra* note 3.
[6] HIPAA Enforcement Statistics Update Service, *supra* note 4. None of the cases that have been prosecuted originated from referrals from the OCR but came from complaints filed by third parties. Remarkably, none of an estimated 24,500 complaints received by OCR through its privacy complaint system resulted in the imposition of civil penalties.
[7] 42 U.S.C. § 1320d-6(a) (emphasis added).
[8] 42 U.S.C. § 1320d-6(b).

individually identifiable health information for some form of personal financial gain by an "employee" of a covered entity.

A federal prosecutor in Seattle, Washington was the first to prosecute a criminal HIPAA violator. The case involved a phlebotomist, Richard Gibson, who was an employee of the Seattle Cancer Care Alliance, a treatment center for cancer patients.[9] Gibson had access to patient information and after obtaining the name, date of birth and social security number of one of the cancer patients, used the information to obtain credit cards in that patient's name.[10] Gibson used several of the credit cards to receive cash advances and to purchase various items, including video games, home improvement supplies, apparel, jewelry and gasoline valued at $9,139.42.[11]

Gibson was charged with wrongful disclosure of individually identifiable health information with the intent to use the information for personal gain in violation of 42 U.S.C. § 1320d-6(a)(3) and § 1320d-6(b)(3)(1).[12] In August 2004, Gibson 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.[13]

In June of 2005, less than a year after the Gibson conviction, the Office of Legal Counsel of the Department of Justice (OLC) issued a Memorandum Opinion clarifying the scope of criminal enforcement under 42 U.S.C. § 1320d-6.[14] This opinion, in response to a joint request from the General Counsel for the Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General,[15] has been interpreted by some to mean that "rank and file" employees of covered entities, like Gibson, are not subject to HIPAA's criminal sanctions.[16]

The OLC opinion specifically addressed the issue of who could be held liable for a HIPAA criminal violation and answered the question of the proof required to establish a "knowing" violation of the HIPAA rules.[17] According to the author of the Opinion, Steven G. Bradbury, Principal Deputy Assistant Attorney General, only covered entities

---

[9] *See* Plea Agreement, United States v. Gibson, No. CR04-0374RSM, 2004 WL 2237585 (W.D. Wash. August 19, 2004).
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *See* Memorandum Opinion for The General Counsel Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General on the Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6 (June 1, 2005), *available at* http://www.usdoj.gov/olc/hipaa_final.htm.
[15] *Id.*
[16] *See* AIS Compliance, *HIPAA Compliance Strategies – HIPAA Criminal Cases Against Individuals Proceed Despite DOJ Memo*, *available at* http://www.aishealth.com/Compliance/Hipaa/RPP_HIPAA_Cases_Proceed.html. *See also* Peter P. Swire, *Justice Department Opinion Undermines Protection of Medical Privacy*, Center for American Progress (June 7, 2005), *available at* http://www.americanprogress.org/issues/2005/06/b743281.html.
[17] *See* Memorandum Opinion, *supra* note 14, at 1.

as defined in §1320d-1 of the Act[18] may be prosecuted directly under 42 U.S.C. § 1320d-6.[19] When the covered entity is not an individual, principles of corporate criminal liability will be used to determine the entity's liability and the potential liability of particular individuals who acted for the entity.[20] Bradbury further stated that the liability of other persons who may not be *directly* liable under § 1320d-6 will be determined in accordance with principles of aiding and abetting liability or of conspiracy liability.[21] Whether this opinion actually means that the HIPAA criminal enforcement provisions do not apply to an "employee" of a covered entity is subject to interpretation and remains unclear.[22]

Since the issuance of the OLC opinion, however, several Federal prosecutors, apparently undeterred by the opinion, have pursued complaints against individual employees of covered entities. In March of 2006 the U.S. Attorney's Office in Houston announced that it had obtained the conviction of a physician practice employee for selling individually identifiable health information.[23] That case, against an Alamo, Texas resident, Liz Arlene Ramirez, likely received the attention of the U.S. Attorney's office because it involved the sale of an FBI agent's individually identifiable health information. At the time in question, Ramirez worked for a physician who had a contract to provide physicals and medical treatment to FBI agents.[24] She became involved with someone whom she thought was working for a drug trafficker and in exchange for $500 provided this person with the medical records of one of the physician's FBI patients.[25] Unbeknownst to her, the person to whom she sold the records was a confidential informant for the FBI.[26]

Ramirez was indicted for knowingly using, obtaining and disclosing individually identifiable health information with the intent to sell, transfer, and use this information for personal gain and malicious harm.[27] After accepting her guilty plea, the court sentenced Ramirez 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.[28] The court found two aggravating factors that incrementally increased her punishment: the fact that Ramirez had sold the confidential medical record and that the records belonged to a federal agent.[29]

---

[18] A "covered entity" is defined in 42 U.S.C. § 132d-1 as a health plan, health care clearinghouse, health care provider who transmits any health information in electronic form in connection with a transaction referred to in § 1320d-2(a)(1) of this title, and a Medicare prescription drug card sponsor. *See* 42 U.S.C. § 1320d-1 (2000) and 42 U.S.C. § 1395w-141(h)(6) (West 2004).
[19] *See* Memorandum Opinion *supra* note 14 at 4.
[20] *Id.*
[21] *Id.*, emphasis added.
[22] *See* HIPAA Compliance Strategies, *supra* note 16; Swire, *supra* note 16.
[23] *See* Press Release, Department of Justice, Alamo Woman Convicted of Selling FBI Agent's Medical Records (Mar. 7, 2006), http://www.usdoj.gov/usao/txs/releases/March2006/060307-Ramirez.pdf.
[24] *Id.*
[25] *Id.*
[26] *Id*.
[27] United States v. Ramirez; No.7:05CR00708 (S.D. Tex. August 30, 2005). *See also* Press Release, *supra* note 11.
[28] *See* Press Release, *supra* note 23.
[29] *See* Press Release, *supra* note 23.

The third and fourth HIPAA criminal prosecutions also involved the theft and sale of individually identifiable health information and led to the first HIPAA criminal case to actually go to trial.[30] According to the indictment, Isis Machado, an employee at the Cleveland Clinic in Weston, Florida, accessed computerized patient files and downloaded individually identifiable health information on more than 1,100 Medicare patients.[31] Machado then sold the information to her cousin, Fernando Ferrer, Jr., the owner of Advanced Medical Claims in Naples, Florida. Ferrer then caused the stolen information to be used in connection with the submission of approximately $2.8 million in fraudulent Medicare claims.[32]

Machado and Ferrer were charged with one count of conspiring to defraud the United States, one count of computer fraud, one count of wrongful disclosure of individually identifiable health information (a HIPAA violation), and five counts of aggravated identity theft.[33] Machado, who pled guilty prior to trial, testified against Ferrer, and a Fort Lauderdale jury convicted Ferrer on all eight counts.[34] Ferrer's sentencing has been scheduled for April 12, 2007, at which time he faces a maximum statutory term of imprisonment of five years on the computer fraud count; ten years on the wrongful disclosure of individually identifiable health information count, and two years on each count of aggravated identity theft.[35]

The paucity of criminal enforcement actions leads one to question whether the system that our government has created to protect patient confidentiality is actually working. Although the Justice Department has successfully convicted four HIPAA criminal violators, the fact that so many other criminal complaints have escaped prosecution raises valid concern for the effectiveness of HIPAA's enforcement provisions. A plausible explanation for this disparity is that the DOJ, although not completely giving up, simply does not want to deal with the barriers created by the OLC in pursuing HIPAA violations against the primary culprits – employees (of covered entities) – and has, therefore, chosen to focus its efforts elsewhere. If, indeed, this is the explanation for the lack of criminal enforcement activity, then it would behoove the OLC to reconsider its position or, alternatively, for Congress to propose and enact legislation amending the HIPAA rules to clearly provide for application of the criminal enforcement provisions to non-covered entities.

---

[30] *See* Press Release, Federal Bureau of Investigation Miami Field Division, Naples Man Convicted in Cleveland Clinic Identity Medicare Fraud Case (Jan. 24, 2007), *available at* http://miami.fbi.gov/dojpressrel/pressrel07/mm20070124b.htm.

[31] United States v. Ferrer; No. 06-60261 CR-COHN (S.D.Fla. Sept. 7, 2006).

[32] *See* Madeline Baro Diaz, Cousins Face ID Theft and Fraud Charges for Stealing Medical Records, Patient Privacy Rights Foundation E-News (Sept. 9, 2006), *available at* *http://www.patientprivacyrights.org/site/News2?page=NewsArticle&id=*6483. *See also*, Press Release, United States Attorney's Office Southern District of Florida, Two Charged in Computer Fraud, Identity Theft and Health Care Fraud Conspiracy (Sept. 8, 2006), *available at* http://www.usdoj.gov/usao/fls/PressReleases/060908-01.html.

[33] Indictment, *Ferrer*, No.06-60261 CR-COHN.

[34] *See* Press Release, *supra* note 30.

[35] *See* Press Release, *supra* note 30.

February 2007