

Davis Wright Tremaine LLP 

Federal Criminal Enforcement of HIPAA

David V. Marshall
Partner
Davis Wright Tremaine LLP
Bellevue, WA
425-646-6137
davidmarshall@dwt.com

Rebecca L. Williams, R.N., J.D.
Partner
Davis Wright Tremaine LLP
Seattle, WA
206-628-7769
beckywilliams@dwt.com



HIPAA: Enforcement

- **Criminal**
 - Penalties imposed by statute
 - Department of Justice
- **Civil**
 - Primarily controlled by regulation
 - See Enforcement Rule
 - Watchdogs
 - Office for Civil Rights
 - Centers for Medicare and Medicaid Services
- **No private right of action**
 - But see state privacy tort law





HIPAA Offense (42 U.S.C. § 1320d-6)

A person who knowingly and in violation of this part –

- (1) uses or causes to be used a unique health identifier;
- (2) obtains individually identifiable health information relating to an individual; or
- (3) discloses individually identifiable health information to another person.





HIPAA Penalties (42 U.S.C. §1320d-6)

Criminal Penalties for HIPAA Violation

- Can be fined not more than \$50,000, imprisoned not more than 1 year, or both;
- If the offense is committed under false pretenses, can be fined not more than \$100,000, imprisoned not more than 5 years, or both; and
- If the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, can be fined not more than \$250,000, imprisoned not more than 10 years, or both.





Thus, Three HIPAA Crimes

- Federal misdemeanor for “knowing” violation; DOJ says requires knowledge of facts, not knowledge that conduct illegal
- Five year felony if knowing violation involved false pretenses (such as misrepresentation of identity); and
- Ten year felony if a knowing violation involved intent to transfer or use PHI for gain or to cause harm



Similar Crimes: Identity Theft (18 U.S.C. §1028)

- (a)(7) “Whoever . . . knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law, shall be punished . . .
- (c)(3)(A) – “The circumstance referred to in subsection (a) . . . is that – the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means...”



Similar Crimes: Fraudulent Access to Computer (18 U.S.C. § 1030)

- (a)(4) “Whoever – knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1 year period.”
- (a)(6) “Whoever knowingly and with intent to defraud traffics ... in any password or similar information through which a computer may be accessed without authorization if ... such trafficking affects interstate or foreign commerce...”

Similar Crimes: Fraudulent Access to Computer (28 U.S.C. §1030)

- “Protected computer” is one:
(e)(2)(B) “... used in interstate or foreign commerce or communication, including a computer located outside the United States, that is used in a manner that affects interstate or foreign commerce”





Three Criminal Prosecutions Reported to Date

- United States v. Richard W. Gibson
Western District of Washington (Seattle)
Pled guilty August 19, 2004
- United States v. Liz Ramirez
Southern District of Texas (McAllen)
Pled guilty March 6, 2006
- United States v. Fernando Ferrer, Jr. & Isis Machado
Southern District of Florida (Ft. Lauderdale)
Indictment announced September 8, 2006
- And . . . rumors of a New York case





U.S. v. Richard W. Gibson

- Employed by Seattle Cancer Care Alliance
- Obtained name, DOB and SSN of cancer patient
- Applied for credit cards in patient's name
- Charged video games, home improvement supplies, clothes, jewelry, groceries and gasoline
- Total charges: \$9,139.42
- Sentence: 16 months in prison, \$15,569.42 in restitution



U.S. v. Liz Ramirez

- Worked at physician clinic that provided services to FBI agents
- Offered to sell personal and medical info re FBI agent for \$500 to person Ramirez thought worked for a drug trafficker
- Purchaser was working undercover for FBI
- Sentence (August 2006): six months in prison, four months home confinement





U.S. v. Fernando Ferrer, Jr. & Isis Machado

- Machado was a coordinator at a Cleveland Clinic in Naples, Florida
- Per prosecutors, Machado:
 - printed info from electronic files that included DOB, SSN, & addresses about Medicare patients
 - then sold info to her cousin Ferrer, owner of Advanced Medical Claims in Naples
 - info then used to file false Medicare claims, involving 1,100 victims and more than \$2.8 million in claims



U.S. v. Fernando Ferrer, Jr. & Isis Machado

- Both indicted for conspiracy to:
 - wrongfully disclose PHI;
 - commit computer fraud; &
 - commit identity theft
- Also charged with:
 - HIPAA crime of obtaining individually identifiable health information with intent to sell, transfer and use for personal gain (the ten year felony);
 - fraud in connection with computers (18 U.S.C. § 1030);
 - five counts of aggravated identity theft (18 U.S.C. § 1028)



U.S. v. Fernando Ferrer, Jr. & Isis Machado

- Initial appearances in federal court 9/8/2006 & released on bond
- If convicted, Machado and Ferrer could be sentenced to 10 years in prison & fined \$250,000 on most serious charges
- Of course, the charges are merely accusations and the defendants are presumed innocent until proven guilty



DOJ June 1, 2005 Legal Opinion

- Following enactment of HIPAA criminal provisions, regulated community questioned whether the new HIPAA criminal prohibitions applied to anyone other than “covered entities,” that is health care plans, health care clearinghouses, certain health care providers and sponsors of Medicare prescription drug cards
- In response to HHS request for a legal opinion about who was “directly” liable, DOJ’s Office of Legal Counsel issued a letter opinion June 1, 2005

Protect
Patient
Information





DOJ June 1, 2005 Legal Opinion

- Internal memorandum, but leaked and thereafter posted to Internet
- DOJ Office of Legal Counsel opinions not legally binding on judiciary, but bind gov't agencies, including DOJ prosecutors
- DOJ opinion criticized by academics and privacy advocates. One HIPAA expert, a former Chief Counselor for Privacy and the OMB described DOJ opinion as “bad law and bad policy,” based on language of statute and Congressional intent to reach more than “covered entities”



DOJ Opinion (cont'd)

- DOJ opined that analysis of *direct* liability for a HIPAA crime “must begin with covered entities, the only persons to whom the standards [*directly*] apply” (parenthetical added)
- DOJ’s opinion focused on the language of the statute, which *directly* makes criminally liable “a person” who “obtains or discloses” PHI “*in violation of this part*”
 - “this part” means the HIPAA administrative simplification provisions, under which HHS issued the HIPAA rules, applying to “covered entities”



DOJ Opinion (cont'd)

DOJ's opinion further stated that:

“depending on the facts of a given case, certain directors, officers, and employees of these entities may be liable directly under section 1320d-6, in accordance with general principles of corporate criminal liability, as these principles are developed in the course of particular prosecutions.”

“The liability of persons for conduct that may not be prosecuted directly under [HIPAA] will be determined by principles of aiding and abetting liability and of conspiracy liability.”



18 U.S.C. § 2: Aiding, Abetting, & Causing

The federal criminal aiding, abetting and causation statute provides:

(a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.

(b) Whoever willfully causes an act to be done which if directly performed by him or *another* would be an offense against the United States, is punishable as a principal.

(Emphasis added.)



18 U.S.C. §2: “Or Another” Added in 1951 Amendments

Senate Report accompanying 1951 amendment explained purpose:



“This section is intended to clarify and make certain the intent to punish aiders and abettors regardless of the fact that they may be incapable of committing the specific violation which they are charged to have aided and abetted. Some criminal statutes of title 18 are limited in terms to officers and employees of the Government, judges, judicial officers, witnesses, officers or employees or persons connected with national banks or member banks.”



18 U.S.C. § 2: Aiding, Abetting, & Causing

- By adding phrase “or another” to statute in 1951, Congress intended “to . . . make certain the intent to punish (persons embraced within Section 2) . . . regardless of the fact that they may be incapable of committing the specific violation” as a direct matter
- 18 U.S.C. § 2 is codification of common law maxim *qui facit per alium facit per se*, or in English, “He who acts through another, acts himself”
- Via § 2, the federal criminal system holds parties accountable, even if they act through the agency of others



U.S. v. Fernando Ferrer, Jr. & Isis Machado Indictment:

Specifically, defendant **FERNANDO FERRER, JR.**, caused defendant **ISIS MACHADO** to obtain individually identifiable health information relating to an individual, that is, patients' names, dates of birth, Social Security numbers, Medicare numbers, and addresses, which had been collected by the health care provider, with the intent to sell, transfer, and use said information for personal gain.

All in violation of Title 42, United States Code, Sections 1320d-6(a)(2) and (b)(3), and Title

18, United States Code, Section 2.





U.S. v. Scannapieco, 611 F.2d 619 (5th Cir. 1980)

- Fifth Circuit upheld conviction of a *salesman* working for firearms *dealer* based on language of 18 U.S.C. §2(b), because *salesman* “caused” a violation of 18 U.S.C. §922
 - That statute prohibits a *dealer* from selling and delivering firearm(s) to buyer while knowing buyer does not reside in state of sale
- *Salesman’s* conviction upheld despite fact *dealer* was not present at time of illegal sales and not convicted of sales, and despite fact that salesman was not within category of persons prohibited from certain acts under statute
- Other cases support this doctrine; see cases collected at *Annotation*, 52 A.L.R. Fed. 769



Article by DOJ Attorney Peter Winn:

- Analyzing Section 2 and court decisions including Scannapieco, respected DOJ health care prosecutor Peter Winn (from Seattle U.S. Attorney's Office) has opined in a published and widely quoted article:

“So long as the underlying conduct would have constituted an offense if it had been committed directly by the covered entity, the employee of the covered entity who was responsible for the conduct is still subject to prosecution as a principal under Section 2(b).”



18 U.S.C. § 371: Conspiracy

- Citing §371, the DOJ opinion states:
“conspiracy statute prescribes punishment “if two or more persons conspire . . . to commit any offense against the United States . . . and one or more of such persons do any act to effect the object of the conspiracy”
- Federal conspiracy liability very broad, and poses substantial risk to third parties who affiliate with covered entity employees who “cause” entity to violate HIPAA



U.S. v. Fernando Ferrer, Jr. & Isis Machado Indictment:

6. From on or about May 23, 2005, and continuing through on or about June 26, 2006, at Broward County, in the Southern District of Florida, and elsewhere, the defendants,

**FERNANDO FERRER, JR.,
and
ISIS MACHADO,**

did knowingly and willfully combine, conspire, confederate, and agree with each other and with others known and unknown to the Grand Jury, to defraud the United States and to commit certain other offenses against the United States, namely: * * *

c. to knowingly and for a reason other than permitted by Title 42, United States Code, Chapter 7, Subchapter XI, Part C, obtain individually identifiable health information relating to an individual, with the intent to sell, transfer, and use, and cause to be used, individually identifiable health information for personal gain, in violation of Title 42, United States Code, Sections 1320d-6(a)(2) and (b)(3).



HIPAA Internal Investigation; Attorney-Client Privilege



- To protect internal investigation critical to involve counsel
- In-house Counsel
 - Knows organization and its people
 - Knows how to reach personnel to conduct interviews
 - But could be witness and may not be clear what hat worn (lawyer or senior executive)
- Outside Counsel
 - Sends message: Investigation serious
 - Spokesperson if government evaluating whether entity non-feasance responsible
 - Counsel with experience in government investigations can look out for risks to entity



HIPAA Internal Investigation: Essential Tasks

- Secure relevant records
- Interview staff with information about events
- Create and implement remedial actions
- Determine any necessary outside communications; notice to patients required under state law, or will minimize liability?



HIPAA Internal Investigation: Documents



- Relevant documents must be maintained
 - Better to not destroy any documents
- Paper and electronic media
 - Immediately suspend routine recycling backups; generate backup of e-mails and network storage
 - Backup hard drives
 - May need forensic quality data re files; which user had access to files; when accessed



HIPAA Internal Investigation: Documents (cont'd)

- Review relevant documents before interviews
 - May help prioritize order of interviews and identify those who should be interviewed
 - May only have one opportunity to interview (particularly if staff obtain lawyers when investigation starts)
 - Assists in determining role and credibility



HIPAA Internal Investigation: Interview Ground Rules

- Explain who is the client (work for entity)
- Explain communications confidential, to obtain facts to provide legal advice (U.S. v. Upjohn elements for corporate attorney client privilege)
- Privilege belongs to entity not employee
- May need to communicate what was learned to entity management and others
- Client entity or counsel may need to communicate with government



HIPAA Internal Investigations: Interviews

- Determine what protected information was obtained
- How obtained (what needs to be fixed)
- What was done with information; potential for recovery
- What purposes? (facts that show wrongful intent or lack of wrongful intent)
 - Knowingly?
 - False pretenses?
 - Intent for financial gain or malicious harm?
- Document interviews



HIPAA Internal Investigation: Remedial Actions

- Decide if HIPAA problem
- Consider necessary steps, including cooperation with authorities (eligibility for credit for corporate cooperation under government policies)
- Steps to mitigate disclosure





HIPAA Internal Investigation: Remedial Actions

- Evaluate necessity and wisdom of alerting potential victims of the violation (e.g., may reduce loss to victims if monitor credit reports)
 - What protected information disclosed
 - Who received
 - Actions to remedy disclosure and mitigate harm





HIPAA Internal Investigation: Remedial Actions

- **Discipline/admonish/retrain violating employee**
- **Disclosure to government in appropriate cases, and cooperation with authorities with respect to information recovery**
- **Disclosure to others (state authorities, regulatory boards, public statements)**



HIPAA Internal Investigation: Remedial Actions



- **Ensure:**
 - **Policies and data handling systems are adequate and operational**
 - **Staff appropriately trained, with refresher training and regular training for new employees**
 - **Disclosures fully investigated and subject of discipline/retraining**



Davis Wright Tremaine LLP

Questions

