Enforcement of the HIPAA Privacy and Security Rules

Gina Stevens
Legislative Attorney

February 3, 2009

Congressional Research Service
7-5700
www.crs.gov
RL33989

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

The privacy and security of health information is recognized as a critical element of transforming the health care system through the use of health information technology. As part of H.R. 1, the American Recovery and Reinvestment Act of 2009, the 111th Congress is considering legislation to promote the widespread adoption of health information technology which includes provisions dealing with the privacy and security of health records. For further information, see CRS Report RS22760, *Electronic Personal Health Records*, by (name redacted).

P.L. 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), directed HHS to adopt standards to facilitate the electronic exchange of health information for certain financial and administrative transactions. Health plans, health care clearinghouses, and health care providers are required to use standardized data elements and comply with the national standards and regulations. Failure to do so may subject the covered entity to penalties.

The HIPAA Privacy Rule was adopted by HHS as the national standard for the protection of health information. It regulates the use and disclosure of protected health information by health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically; establishes a set of basic consumer protections; permits any person to file an administrative complaint for violations; and authorizes the imposition of civil or criminal penalties. Enforcement of the Privacy Rule began in 2003.

The HIPAA Security Rule was adopted by HHS as the national standard for the protection of electronic health information. It requires covered entities to maintain administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information; to protect against any reasonably anticipated threats or hazards to the security or integrity of such information, as well as protect against any unauthorized uses or disclosures of such information. The Centers for Medicare and Medicaid Services (CMS) has been delegated authority to enforce the HIPAA Security Standard, effective February 16, 2006.

On March 16, 2006, the Final HIPAA Administrative Simplification Enforcement Rule became effective. The Enforcement Rule has both procedural and substantive provisions, and is applicable to all HIPAA administrative simplification standards. The Enforcement Rule establishes procedures for the imposition of civil money penalties for violations of the rules.

Lawmakers and others are examining the statutory and regulatory framework for enforcement of the HIPAA Privacy and Security standards, and ways to ensure that agencies use their enforcement authority under HIPAA to address improper uses and disclosures of protected health information. Concerns have been raised by some that the HIPAA Privacy and Security Rules are being under enforced by HHS, DOJ, and CMS. Of approximately 41,107 health information privacy complaints filed with HHS since 2003, HHS found authority to investigate and resolve 7,729 cases. Criminal convictions have been obtained by DOJ in four cases involving employees of covered entities who improperly obtained protected health information. Since February 2006, CMS has not conducted any HIPAA Security Rule compliance reviews.

This report provides an overview of the HIPAA Privacy and Security Rules, and of the statutory and regulatory enforcement scheme. In addition, it summarizes enforcement activities by HHS, DOJ, and CMS. This report will be updated.

Contents

Contacts

Introduction

The privacy and security of health information is recognized as a critical element of transforming the health care system through the use of health information technology. As part of H.R. 1, the American Recovery and Reinvestment Act of 2009, the 111th Congress is considering legislation to promote the widespread adoption of health information technology (HIT), and the bill includes provisions dealing with the privacy and security of health records, and specifically authorizes state attorneys general to file lawsuits in federal court on behalf of state residents, seeking injunctive relief or civil damages against "any person" who violates HIPAA's privacy provisions.[1]

The Health Insurance Portability and Accountability Act of 1996

In 1996, Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[2] to "improve portability and continuity of health insurance coverage in the group and individual markets."[3] Congress enacted HIPAA to guarantee the availability and renewability of health insurance coverage and limit the use of pre-existing condition restrictions. HIPAA also included tax provisions related to health insurance and administrative simplification provisions requiring issuance of national standards to facilitate the electronic transmission of health information.

National Standards

Part C of HIPAA[4] requires "the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[5] Such standards are required to be consistent with the objective of reducing the administrative costs of providing and paying for health care.

These Administrative Simplification provisions require the Secretary of HHS to adopt national standards to facilitate the electronic exchange of information for certain financial and administrative transactions; select or establish code sets for data elements; protect the privacy of individually identifiable health information; maintain administrative, technical, and physical safeguards for the security of health information; provide unique health identifiers for individuals, employers, health plans, and health care providers; and to adopt procedures for the use of electronic signatures.[6]

---

[1] See CRS Report R40161, *The Health Information Technology for Economic and Clinical Health (HITECH) Act*, by (name redacted); and Markle Foundation, *Health IT Investments that Improve Healthcare: Critical Information Policy and Technology Attributes and Expectations*, January 2009, at http://www.markle.org/events/20090113_transition/20090113_health_it_investments.pdf.

[2] P.L. 104-191, 110 Stat. 1936 (1996), codified in part at 42 U.S.C. §§ 1320d *et seq.*

[3] H.Rept. 104-496, at 1, 66-67, reprinted in 1996 U.S.C.C.A.N. 1865, 1865-66.

[4] 42 U.S.C. §§ 1320d—1320d-8.

[5] 110 Stat. 2021.

[6] 42 U.S.C. §§ 1320d-2(a)-(d). HHS has issued final regulations to adopt national standards for transactions and code sets, privacy, security, and employer identifiers. *See Administrative Simplification Under HIPAA: National Standards for Transactions, Privacy and Security*, at http://www.hhs.gov/news/press/2002pres/hipaa.html.

Health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically are required to use standardized data elements and comply with the national standards and regulations promulgated pursuant to Part C.[7] Failure to comply with the regulations may subject the covered entity to civil or criminal penalties.

Civil Money Penalties

Under HIPAA, the Secretary is required to impose a civil monetary penalty (CMP) on any person failing to comply with the Administrative Simplification provisions in Part C.[8] The maximum civil money penalty (i.e., the fine) for a violation of an administrative simplification provision is $100 per violation and up to $25,000 for all violations of an identical requirement or prohibition during a calendar year.[9]

A number of procedural requirements that are relevant to the imposition of CMP's for violations of the Administrative Simplification standards[10] are incorporated by reference in HIPAA from the general civil money penalty provision in 42 U.S.C. § 1320a-7a.[11] The Secretary may not initiate a CMP action "later than six years after the date" of the occurrence that forms the basis for the CMP action.[12] The Secretary may initiate a CMP by serving notice in a manner authorized by Rule 4 of the Federal Rules of Civil Procedure (Commencement of Action). The Secretary must give written notice to the person on whom he wishes to impose a CMP and an opportunity for a determination to made "on the record after a hearing at which the person is entitled to be represented by counsel, to present witnesses, and to cross-examine witnesses against the person."[13] Judicial review of the Secretary's determination and the issuance and enforcement of subpoenas is available in the United States Court of Appeals.[14]

A CMP may not be imposed with respect to an act that constitutes criminal disclosure of individually identifiable information[15] "if it is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provisions";[16] or if "the failure to comply was due to reasonable cause and not to willful neglect" and is corrected within 30 days after learning of the violation.[17] The Secretary may provide technical assistance during such period. A CMP may be

[7] 42 U.S.C. § 1320d-4(b) Requires compliance with the regulations within a certain time period by "each person to whom the standard or implementation specification [adopted or established under sections 1320d-1 and 1320d-2] applies."

[8] 42 U.S.C. § 1320d-5(a).

[9] 42 U.S.C. § 1320d-5(a)(1).

[10] 42 U.S.C. § 1320d-5(a)(2).

[11] Except for the subsections addressing the imposition of civil money penalties for improperly filed claims, payments to induce a reduction or limitation of services, and the recovery and use of funds.

[12] 42 U.S.C. § 1320a-7a(c)(1).

[13] 42 U.S.C. § 1320a-7a(c)(2).

[14] 42 U.S.C. § 1320a-7a(e).

[15] 42 U.S.C. § 1320d-5(b)(1).

[16] 42 U.S.C. § 1320d-5(b)(2).

[17] 42 U.S.C. § 1320d-5(b)(3).

reduced or waived "to the extent that the payment of such penalty would be excessive relative to the compliance failure involved."[18]

Three specific affirmative defenses bar the imposition of civil money penalties: (1) the act is a criminal offense under HIPAA's criminal penalty provision—wrongful disclosure of individually identifiable health information; (2) the covered entity did not have actual or constructive knowledge of the violation; and (3) the failure to comply was due to reasonable cause and not to willful neglect, and the failure to comply was corrected during a 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.[19]

The Office of Civil Rights (OCR) in HHS is responsible for enforcing the Privacy Rule.[20] OCR has said that any civil penalties imposed will only affect covered entities; in other words, a member of a workforce who is not a covered entity appears not to be subject to civil sanctions by OCR.

Criminal Penalties

HIPAA establishes criminal penalties for any person who knowingly and in violation of the Administrative Simplification provisions of HIPAA uses a unique health identifier or obtains or discloses individually identifiable health information.[21] Enhanced criminal penalties may be imposed if the offense is committed under false pretenses, with intent to sell the information or reap other personal gain.

The penalties include (1) a fine of not more than $50,000 and/or imprisonment of not more than 1 year; (2) if the offense is "under false pretenses," a fine of not more than $100,000 and/or imprisonment of not more than 5 years; and (3) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10

---

[18] 42 U.S.C. § 1320d-5(b)(4).

[19] 42 U.S.C. § 1320d-5(b)(1)—(4).

[20] 65 Fed. Reg. 82381.

[21] 42 U.S.C. § 1320d-6(a). Wrongful disclosure of individually identifiable health information

(a) Offense

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,

shall be punished as provided in subsection (b) of this section.

(b) Penalties

A person described in subsection (a) of this section shall—

(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;

(2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and

(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both. 42 U.S.C. § 1320d-6.

years.[22] These penalties do not affect any other penalties that may be imposed by other federal programs.

Scope of Criminal Enforcement

In 2005, the Justice Department Office of Legal Counsel (OLC) addressed which persons may be prosecuted under HIPAA.[23] Based on its reading of the plain terms of the statute, the privacy regulations, and Executive Order 13,141 (To Protect the Privacy of Protected Health Information in Oversight Investigations), OLC concluded that only a covered entity could be criminally liable "in violation of this part."[24] Because Part C applies only to covered entities and mandates compliance only by covered entities, OLC concluded that direct liability for violations of section 1320d-6 was limited to covered entities (health plans, health care clearinghouses, those health care providers specified in the statute, and Medicare prescription drug card sponsors); and depending on the facts of a given case, certain directors, officers, and employees of these entities may be liable directly under section 1320d-6, based on general principles of corporate criminal liability.[25] Other persons who obtain protected health information in a manner that causes a covered entity to release the information in violation of HIPAA, including recipients of protected information, may not be liable directly. The liability of persons for conduct that may not be prosecuted directly under section 1320d-6 is to be determined by principles of aiding and abetting liability under 18 U.S.C. § 2[26] and of conspiracy liability under 18 U.S.C. § 371.[27] OLC also noted that such conduct may also be punishable under other federal laws, such as the identity theft under 18 U.S.C. § 1028[28] and fraudulent access of a computer under 18 U.S.C. § 1030.[29]

---

[22] 42 U.S.C. § 1320d-6(b).

[23] U.S. Department of Justice, *Scope of Criminal Enforcement Under 42 U.S.C. §1320d-6*, June 1, 2005 at http://www.justice.gov/olc/hipaa_final.htm.

[24] OLC's opinion limiting direct liability under the HIPAA criminal statute to covered entities was widely criticized. Critics believed that such an interpretation would result in weak enforcement of the HIPAA standards. *See* Robert Pear, *Ruling Limits Prosecutions of People Who Violate Law on Medical Records*, *New York Times* (June 7, 2005); Peter P. Swire, *Justice Department Opinion Undermines Protection of Medical Privacy*, Center for American Progress (June 7, 2005), at http://www.americanprogress.org/issues/2005/06/b743281.html; Peter A. Winn, *Who Is Subject to Criminal Prosecution under HIPAA?*, at

http://www.abanet.org/health/01_interest_groups/01_media/WinnABA_2005-11.pdf.

[25] According to OLC under general principles of corporate criminal liability, the conduct of an entity's agents may be imputed to the entity when the agents act within the scope of their employment, and the criminal intent of agents may be imputed to the entity when the agents act on its behalf.

[26] § 2. Principals

(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.

[27] § 371. Conspiracy to commit offense or to defraud United States

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.

If, however, the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor.

[28] See CRS Report RL31919, *Federal Laws Related to Identity Theft*, by Gina Marie Stevens.

[29] See CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by (name redacted).

The Office of Legal Counsel also considered what the "knowingly" element of the offense requires and concluded that the "knowingly" element is best read, consistent with its ordinary meaning, to require only proof of knowledge of the facts that constitute the offense.[30]

The HIPAA Privacy Rule

To carry out the requirements of Part C, the HIPAA Privacy Rule, 45 C.F.R. Parts 160 and 164,[31] was adopted as the national standard for the protection of individually identifiable health information.[32] Enforcement of the Privacy Rule began on April 14, 2003, except that for small health plans with annual receipts of $5 million or less enforcement began April 2004. The Office of Civil Rights (OCR) in HHS is responsible for enforcing the Privacy Rule.[33] The Centers for Medicare and Medicaid Services (CMS) has delegated authority to enforce the non-privacy HIPAA standards, including the Security Rule.[34]

Because of the explicit language of HIPAA, the Privacy Rule applies only to a specified set of "covered entities": (1) health plans, (2) health care clearinghouses, and (3) health care providers who transmit information in electronic form in connection with standard transactions governed by the Administrative Simplification provisions.[35] Medicare prescription drug sponsors were added to the list of "covered entities" in 2003.[36] Excluded from the definition of covered entities are employees of covered entities. Business associates of covered entities are subject to certain aspects of the Privacy Rule.[37]

The Privacy Rule applies to protected health information that is individually identifiable health information "created or received by a health care provider, health plan, or health care clearinghouse" that "[r]elates to the ... health or condition of an individual" or to the provision of or payment for health care.[38]

The HIPAA Privacy Rule[39] governs the use and disclosure of protected health information by HIPAA-covered entities (health plans, health care providers, and health care clearinghouses). The

[30] U.S. Department of Justice, *Scope of Criminal Enforcement Under 42 U.S.C. §1320d-6*, June 1, 2005, at http://www.justice.gov/olc/hipaa_final.htm.

[31] Available at http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=cb27f1d82e0aa82e6671a33a6f589c9f&rgn=div5&view=text&node=45:1.0.1.3.72&idno=45.

[32] The Privacy Rule went into effect on April 14, 2001. On August 14, 2002, HHS published a modified Privacy Rule. 67 Fed. Reg. 53181 available at http://www.hhs.gov/ocr/hipaa/finalreg.html.

[33] The Secretary of Health and Human Services recently delegated to the Director of OCR the authority to issue subpoenas in investigations of alleged violations of the HIPAA Privacy Rule. 72 Fed. Reg. 18,999 (April 16, 2007).

[34] 68 Fed. Reg. 60694.

[35] 42 U.S.C. §§ 1320d-1(a)(1)-(3) ("Any standard adopted under this part shall apply, in whole or in part, to the following persons: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1320d-2(a)(1) of this title.").

[36] 42 U.S.C. § 1320d-1(a); 45 C.F.R. §§ 164.104(a)(1)-(3). The Medicare Prescription Drug Improvement and Modernization Act of 2003, P.L. 108-173, § 101(a)(2), 117 Stat. 2071, 2144 (2003), codified at 42 U.S.C. § 1395w-14(h)(6).

[37] 45 C.F.R. § 164.530(e)(2)(ii)(A).

[38] 45 C.F.R. § 160.103.

[39] 45 C.F.R. § 160 and 164.

Rule requires a covered entity to obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.[40] A covered entity is required to disclose protected health information in two situations: (1) to individuals when they request access to or an accounting of disclosures of their protected health information; and (2) to HHS for compliance review or enforcement action. The HIPAA Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or consent, for 12 national priority purposes.[41]

The HIPAA Security Rule

Regulations governing security standards under HIPAA require health care covered entities to maintain administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information; to protect against any reasonably anticipated threats or hazards to the security or integrity of such information, as well as protect against any unauthorized uses or disclosures of such information.[42] The Centers for Medicare and Medicaid Services (CMS) has been delegated authority to enforce the HIPAA Security Standard.[43]

Effective on February 16, 2006, the Department of Health and Human Services delegated to CMS the authority and responsibility to interpret, implement, and enforce the HIPAA Security Rule provisions; to conduct compliance reviews and investigate and resolve complaints of HIPAA Security Rule noncompliance; and to impose civil monetary penalties for a covered entity's failure to comply with the HIPAA Security Rule provisions.

The Security Rule applies only to protected health information in electronic form (EPHI), and requires a covered entity to ensure the confidentiality, integrity, and availability of all EPHI the covered entity creates, receives, maintains, or transmits. Covered entities must protect against any reasonably anticipated threats or hazards to the security or integrity of such information, and any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule; and ensure compliance by its workforce.[44]

The Security Rule allows covered entities to consider such factors as the cost of a particular security measure, the size of the covered entity involved, the complexity of the approach, the technical infrastructure and other security capabilities in place, and the nature and scope of potential security risks. The Rule establishes "standards" in three categories—administrative, physical, and technical—that covered entities must meet, accompanied by implementation specifications for each standard.

The Security Rule requires covered entities to enter into agreements with business associates who create, receive, maintain or transmit EPHI on their behalf. Under such agreements, the business

[40] 45 C.F.R. § 164.508.

[41] 45 C.F.R. 164.512.

[42] HIPAA Security Standards for the Protection of Electronic Personal Health Information, 45 C.F.R. Part 164.302 *et seq*.

[43] See generally, Centers for Medicare and Medicaid Services, *Security Materials* at http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp#TopOfPage.

[44] 45 C.F.R. § 164.306(a).

associate must: implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the covered entity's electronic protected health information; ensure that its agents and subcontractors to whom it provides the information do the same; and report to the covered entity any security incident of which it becomes aware. The contract must also authorize termination if the covered entity determines that the business associate has violated a material term. A covered entity is not liable for violations by the business associate unless the covered entity knew that the business associate was engaged in a practice or pattern of activity that violated HIPAA, and the covered entity failed to take corrective action.

The HIPAA Administrative Simplification Enforcement Rule

On February 16, 2006, HHS published the Final Enforcement Rule, with both procedural and substantive provisions, applicable to all HIPAA administrative simplification standards in Part C.[45] The final rule went into effect March 16, 2006. The following discussion summarizes the main provisions of the Enforcement rule.

Voluntary Cooperation

With respect to ascertaining compliance with and enforcement of the administrative simplification provisions, the Secretary of HHS is to seek the voluntary cooperation of covered entities. Enforcement and other activities to facilitate compliance include the provision of technical assistance, responding to questions, providing interpretations and guidance, responding to state requests for preemption determinations, and investigating complaints and conducting compliance reviews.

Complaints to the Secretary

The Privacy Rule permits any person to file an administrative complaint for violations.[46] It did not create a private right of action for individuals to sue to remedy privacy violations.[47] Individuals must direct their complaints to the HHS Office for Civil Rights (OCR) or to the covered entity.[48] An individual may file a compliant with the Secretary if the individual believes that the covered entity is not complying with the administrative simplification provisions.[49] Complaints to the Secretary may be filed only with respect to alleged violations occurring on or after April 14, 2003. The Secretary's investigation may include a review of the policies,

[45] 71 Fed. Reg. 8390, 45 CFR § 160.300 *et seq.*

[46] 45 CFR § 160.306.

[47] Several federal district courts have held that HIPAA did not create a privately enforceable right of action, and one federal appellate court has also upheld that finding. *See Acara v. Banks*, 470 F.3d 569 (5th Cir. 2006).

[48] OCR maintains a website with information on the regulation, including guidance at http://www.hhs.gov/ocr/hipaa/. HHS also issued a 20-page "Summary of the HIPAA Privacy Rule," at http://www.hhs.gov/ocr/privacysummary.pdf.

[49] 45 CFR § 160.306.

procedures, or practices of the covered entity, and of the circumstances regarding the alleged acts or omissions.[50]

Compliance Reviews

The Secretary is also authorized to conduct compliance reviews.[51] According to OCR, it is conducting Privacy Rule compliance reviews only where compelling and unusual circumstances demand.[52]

Responsibilities of Covered Entities

Covered entities are required to provide records and compliance reports to the Secretary to determine compliance, and to cooperate with complaint investigations and compliance reviews.[53]

Secretarial Action

In cases where no violation is found, the Secretary is to inform the covered entity and the complainant in writing. In cases where an investigation or compliance review has indicated noncompliance, the Secretary is to inform the covered entity and the complainant in writing, and attempt to resolve the matter informally.[54] If the Secretary determines that the matter cannot be resolved informally, the Secretary may issue written findings documenting the noncompliance. The covered entity has 30 days to respond to the Secretary's findings and must be given an opportunity to submit written evidence of any mitigating factors or affirmative defenses, as it proceeds to the civil monetary penalty phase. Finally, the Rule includes a provision that prohibits covered entities from threatening, intimidating, coercing, discriminating against, or taking any other retaliatory action against anyone who complains to HHS or otherwise assists or cooperates in the HIPAA enforcement process.[55] Actions must be brought by the Secretary within six years from the date of the violation.

Affirmative Defenses

Three specific affirmative defenses would bar the imposition of civil money penalties: (1) the violation is a criminal offense under HIPAA—wrongful disclosure of individually identifiable health information; (2) the covered entity did not have actual or constructive knowledge of the violation; or (3) the failure to comply was due to reasonable cause and not to willful neglect, and

[50] The Secretary has delegated to the Office for Civil Rights (OCR) the authority to receive and investigate complaints as they may relate to the Privacy Rule. 65 Fed. Reg. at 82,474, 82,487.

[51] 45 CFR § 160.308.

[52] U.S. Department of Health and Human Services, Fiscal Year 2008, Office for Civil Rights, *Justification of Estimates for Appropriations Committees*, p. 37, at http://www.hhs.gov/ocr/CJFY2008.pdf. For more recent information on the activities of OCR, see, Fiscal Year 2009 Justification of Estimates for Appropriations Committees at http://www.hhs.gov/ocr/CJ2009.pdf.

[53] 45 CFR § 160.310.

[54] 45 CFR § 160.312. Presumably it was pursuant to this authority that HHS entered into the resolution agreement with Providence Health & Services.

[55] 45 CFR § 160.316.

was corrected during a 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.[56] With respect to the first two defenses, the Secretary may waive the civil money penalty if it would be excessive in relation to the violation.

Civil Money Penalties

The Enforcement rule provides that the "Secretary will impose a civil money penalty upon a covered entity if the Secretary determines that the covered entity has violated an administrative simplification provision."[57]

The Secretary is required to provide notice of a proposed penalty to the covered entity, including the respondent a right to request a hearing within 90 days before an Administrative Law Judge.[58] If the respondent fails to request a hearing, the Enforcement Rule states that "the Secretary will impose the proposed penalty or any lesser penalty permitted by 42 U.S.C. 1320d-5."[59] Once a penalty has become final, the Secretary is obligated to notify the public, state, and local medical and professional organizations; state agencies administering health care programs; utilization and quality peer review organizations; and state and local licensing agencies and organizations.

To determine the number of "violations" to compute the amount of the civil penalty, the Secretary is to base the decision upon the nature of the covered entity's obligation to act or not under the violated provision.[60] The Rule also provides that HHS may consider the following aggravating or mitigating factors when determining the amount of the penalty: the nature of the violation; the circumstances under which the violation occurred; the degree of culpability; any history of prior compliance, including violations; the financial condition of the covered entity; and such "other matters as justice may require."[61] The Secretary is authorized to settle any issue or case or to compromise any penalty.

Criminal Referrals

HHS refers to the DOJ for criminal investigation appropriate cases involving the knowing disclosure or obtaining of individually identifiable health information in violation of the Privacy Rule.

[56] 45 CFR § 160.410.

[57] 45 CFR § 160.402.

[58] Provision is also made for an administrative appeal of the ALJ's decision to the HHS Departmental Appeals Board, and judicial review of the Board's final decision.

[59] 45 CFR § 160.422.

[60] 45 CFR § 160.406.

[61] 45 CFR § 160.408.

DOJ Criminal Enforcement Actions

Criminal convictions have been obtained in four cases involving employees of covered entities who improperly obtained protected health information. Three of the HIPAA criminal cases were brought after the OLC legal opinion limiting direct liability for violations to covered entities.[62]

United States v. Gibson

The first case prosecuted by a U.S. Attorney's Office under the HIPAA criminal statute involved a Seattle phlebotomist employed at a cancer center who was sentenced to 16 months in prison and 3 years of supervised release in 2004 for stealing credit card information from a cancer patient, charging $9,000 worth of merchandise on it, and using that information to get credit cards in the defendant's name.[63] The defendant was ordered to pay restitution in the amount of $15,000. The U.S. attorney's office in Seattle chose to prosecute the identity theft as a criminal HIPAA violation because the information had been collected from a patient,[64] instead of prosecuting the defendant for identity theft.[65] Specifically, the defendant was charged with and pled guilty to the wrongful disclosure of individually identifiable health information for economic gain in violation of 42 U.S.C. § 1320d-6(a)(3) and (b)(3). It is notable that the defendant was not a covered entity but a member of the covered entities workforce not acting within the scope of his employment. The OLC legal opinion was issued after the defendant's conviction.

United States v. Ramirez

In 2006, a Texas woman employed in the office of a doctor who had a contract to provide physicals and medical treatment to FBI agents was convicted of selling an FBI agent's medical records for $500.[66] The defendant pled guilty to the federal felony offense of wrongfully using a unique health identifier intending to sell individually identifiable health information for personal gain, 42 U.S.C. § 1320d-6(a)(1) and (b)(3), and of violating 18 U.S.C. §2.[67] She was sentenced to six months in jail and four months of home confinement to be followed by a two-year term of supervised release.[68] The defendant was also ordered to pay a criminal money penalty of $100.

---

[62] Atlantic Information Services, Inc., *HIPAA Criminal Cases Against Individuals Proceed Despite DOJ Memo*, at http://www.aishealth.com/Compliance/Hipaa/RPP_HIPAA_Cases_Proceed.html

[63] *United States v. Gibson*, 2004 WL 2237585 (No. CR04-0374RSM) (W.D. Wash. 2004).

[64] *See* ABA Health *e*Source, Interview with Susan Loitz, Assistant U.S. Attorney (October 2004), at http://www.abanet.org/health/esource/vol1no2/loitz.html.

[65] *See* Atlantic Consulting Services, Inc., *Synergy Between the Identity Theft Issue And Privacy, Security Grows Stronger*, at http://www.aishealth.com/Compliance/Hipaa/RPP_identity_patient_ID_theft.html. (Noting that "Identity theft is now the number one financial crime in the country, and health care organizations are prime targets because of their vast reservoirs of personal data, such as Social Security numbers.")

[66] *United States v. Ramirez*, Warrant, Criminal No. M-05-708, McAllen Division (S.D. Tex. 2006).

[67] § 2. Principals

(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.

[68] U.S. Department of Justice, *Alamo, Texas Woman Convicted of Selling FBI Agent's Medical Record Sentenced*, at http://www.usdoj.gov/usao/txs/releases/March2006/060307-Ramirez.pdf.

Two aggravating factors were found by the court. First, the defendant had sold the confidential medical record, and second, the record belonged to a federal agent.

United States v. Ferrer and Machado

The defendant was an employee of a medical clinic and improperly obtained Medicare information and other patient information for more than 1,100 clinic patients and sold that information to the owner of a medical claims business for $5 to $10 each. The information was then used by medical providers to fraudulently bill Medicare for services not rendered and equipment not supplied, resulting in a $7 million fraud to Medicare and the payment of approximately $2.5 million to providers and suppliers.[69] The defendants were charged with conspiracy in violation of 18 U.S.C. § 371, with computer fraud in violation of 18 U.S.C. § 1030(a)(4)and (c)(3)(A), wrongful disclosure of individually identifiable health information in violation of 42 U.S.C. § 1320d-6(a)(2) and (b)(3), and aggravated identity theft in violation of 18 U.S.C. § 1028A(a)(2). Because the clinic-employer was a cooperating witness and the defendant was acting outside the scope of her lawful employment, the clinic was not charged.

In January 2007, Florida defendant Machado pled guilty to conspiracy to commit computer fraud, conspiracy to commit identity theft and conspiracy to wrongfully disclose individually identifiable health information.[70] The defendant testified against her co-defendant. The defendant was sentenced on April 27, 2007, and faced a maximum of 5 years imprisonment, $250,000 fine, and possible restitution. Defendant Machado was sentenced to 3 years probation, including 6 months of home confinement, and also ordered to pay restitution in the amount of $2,505,883.

Co-defendant Ferrer, owner of the medical claims business, was convicted by a jury of all eight counts (one count of conspiring to defraud the United States, one count of computer fraud, one count of wrongful disclosure of individually identifiable health information, and five counts of aggravated identity theft).[71] Defendant Ferrer was also sentenced on April 27, 2007, and faced a maximum statutory term of imprisonment of 5 years on the conspiracy count; a maximum statutory term of imprisonment of 5 years on the computer fraud count; a maximum statutory term of imprisonment of 10 years on the wrongful disclosure of individually identifiable health information count; and a maximum statutory term of imprisonment of 2 years on each count of aggravated identity theft. Ferrer was sentenced to 87 months in prison, 3 years of supervised release, and ordered to pay restitution in the amount of $2,505,883. According to DOJ, this is the first HIPAA violation case that has gone to trial.[72] The two other cases resulted in guilty pleas.

United States v. Smith

The defendant, a licensed practical nurse at the time of the crime, pleaded guilty in April, 2008 to wrongfully disclosing individually identifiable health information for personal gain, a violation of

[69] The United States Attorney's Office Southern District of Florida, *Cleveland Clinic Employee Pleads Guilty to Superseding Fraud Indictment*, January 11, 2007, at http://www.usdoj.gov/usao/fls/PressReleases/070111-03.html.

[70] *United States v. Ferrer and Machado*, 2006 WL 4005632 (S.D.Fla. 2006).

[71] The United States Attorney's Office Southern District of Florida, *Naples Man Convicted In Cleveland Clinic Identity Theft and Medicare Fraud Case*, January 24, 2007, at http://www.usdoj.gov/usao/fls/PressReleases/070124-02.html.

[72] *Id.*

the health information privacy provisions of HIPAA.[73] On December 3, 2008, the defendant was sentenced to two years probation including 100 hours of community service.[74]

HHS Enforcement of the HIPAA Privacy Rule

According to recently released data from HHS, from April 2003, when enforcement of the Privacy Rule began, to December 31, 2008, approximately 41,107 health information privacy complaints were filed with HHS.[75] In 23,466 cases, HHS did not find enforcement authority under HIPAA.[76] HHS found authority to investigate and resolve 7,729 cases. In those cases, HHS obtained changes in the investigated entity's privacy practices or other corrective actions.[77] HHS found no violation of the Privacy Rule in 3,858 cases.[78] Almost 6,054 cases remained unresolved.

According to HHS, the compliance issues most frequently investigated were for impermissible use or disclosure of protected health information, lack of adequate safeguards for protected health information, lack of patient access to his or her protected health information, the disclosure of more information than is minimally necessary to satisfy a particular request for information, and failure to have an individual's authorization for a disclosure that requires one.[79] The covered entities most commonly required to take corrective action by HHS, in order of frequency, include private practices, general hospitals, outpatient facilities, health plans, and pharmacies.[80]

According to its enforcement website, HHS did not report any civil penalties during the five-year period of 2003-2008.[81] HHS reported that more than 448 cases were referred by HHS to DOJ for criminal investigation of knowing disclosure or access to protected health information in violation of the Privacy Rule. An additional 285 cases were referred to the Centers for Medicare and Medicaid Services (CMS) for investigation of cases that involve a potential violation of the HIPAA Security Rule. Although information on criminal convictions was not reported by HHS,

[73] U.S. Department of Justice, United States Attorney; Eastern District of Arkansas, *Nurse Pleads Guilty to HIPAA Violation*, April 15, 2008, at http://littlerock.fbi.gov/dojpressrel/pressrel08/hipaaviol041508.htm.

[74] U.S. Department of Justice, United States Attorney, Eastern District of Arkansas, *Nurse Sentenced For HIPAA Violation*, April 15, 2008, at http://www.usdoj.gov/usao/are/news_releases/2008/December/SmithLPN%20sent%20HIPAA%20120308.pdf.

[75] U.S. Department of Health and Human Services, *Enforcement Highlights*, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html.

[76] *Id.* Either because of lack of jurisdiction (the violation occurred prior to the effective date of the Rule or the entity was not subject to the Privacy Rule); the complaint was untimely, withdrawn, or not pursued by the complainant; or the activity being complained of did not violate the Privacy Rule.

[77] Id.

[78] Id.

[79] *See* U.S. Department of Health and Human Services, *Most Investigated Compliance Issues*, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html.

[80] *See* U.S. Department of Health and Human Services, *Most Common Types of Covered Entities Required to Take Corrective Action*, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html.

[81] The U.S. Department of Health and Human Services (HHS) recently announced an enhanced website to make it easier to get information about how the Department enforces health information privacy rights and standards. In addition, the Office Of Civil Rights launched a redesigned website on January 16, 2009, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html.

criminal convictions were obtained in four cases involving employees of covered entities who improperly obtained protected health information.[82]

Concerns have been raised by some that the HIPAA Privacy Rule is being underenforced by the U.S. Departments of Health and Human Services (HHS) and Justice (DOJ).[83] Privacy advocates have been critical of HHS' enforcement of the HIPAA Privacy Rule which has focused on technical assistance and voluntary cooperation for the covered entity with HHS. According to HHS, several factors contribute to the number of enforcement actions taken by it for violations of the HIPAA Privacy Rule. First is HHS's preference for voluntary compliance, corrective action, and/or resolution agreement.[84] Second, HIPAA applies only to certain groups, defined as covered entities, health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically. HIPAA does not cover all types of entities that maintain personal health information (e.g., life insurers, employers, workers compensation carriers, schools and school districts, state agencies such as child protective service agencies, law enforcement agencies, and municipal offices).[85] Third, HIPAA does not cover of all types of health transactions. Fourth, the statute does not create a private right of action, but rather public enforcement by HHS and DOJ. Fifth, the complained-of activity might not be a violation of the Privacy Rule.

In July 2008, the first time since the Privacy Rule went into effect in 2003, HHS required a resolution agreement from a covered entity (a contract signed by HHS and the covered entity) for violations of the HIPAA Privacy and Security Rules.[86] HHS entered into a resolution agreement with Providence Health & Services requiring the covered entity to pay $100,000 and to implement a corrective action plan to safeguard identifiable electronic patient information to settle potential violations of the HIPAA Privacy and Security Rules. In this case the violations involved the loss of backup tapes and theft of laptops containing individually identifiable health information.

CMS Enforcement of the HIPAA Security Rule

The Centers for Medicare & Medicaid Services (CMS) is the agency within HHS that is responsible for enforcing the HIPAA Security Rule. In October 2008, the HHS inspector general released a report on the results of his audit to evaluate the effectiveness of CMS's oversight and enforcement of covered entities' implementation of the HIPAA Security Rule. Inspector General Daniel R. Levinson concluded that

[82] *United States v. Gibson*, 2004 WL 2237585 (No. CR04-0374RSM) (W.D. Wash. 2004); *United States v. Ramirez*, Warrant, Criminal No. M-05-708, McAllen Division (S.D. Tex. 2006); *United States v. Ferrer and Machado*, 2006 WL 4005632 (S.D.Fla. 2006).

[83] Rob Stein, "Medical Privacy Law Nets No Fines," *The Washington Post*, June 5, 2006 at A01.

[84] U.S. Department of Health and Human Services, *Compliance and Enforcement: How OCR Enforces the HIPAA Privacy Rule*, at http://www.hhs.gov/ocr/privacy/enforcement/hipaarule.html.

[85] HHS's approach to the regulation of the privacy of health information "is also significantly informed by the limited jurisdiction conferred by HIPAA. In large part, we have the authority to regulate those who create and disclose health information, but not many key stakeholders who receive that health information from a covered entity." 65 Fed. Reg. 82462, 82471 (2000).

[86] *See, Resolution Agreement*, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/agreement.pdf.

> CMS had taken limited actions to ensure that covered entities adequately implement the HIPAA Security Rule. These actions had not provided effective oversight or encouraged enforcement of the HIPAA Security Rule by covered entities. Although authorized to do so by Federal regulations as of February 16,2006, CMS had not conducted any HIPAA Security Rule compliance reviews of covered entities. To fulfill its oversight responsibilities, CMS relied on complaints to identify any noncompliant covered entities that it might investigate. As a result, CMS had no effective mechanism to ensure that covered entities were complying with the HIPAA Security Rule or that ePHI was being adequately protected.[87]

Although CMS did not agree with those findings, the inspector general recommended that CMS establish policies and procedures for conducting HIPAA Security Rule compliance reviews of covered entities.

Author Contact Information

(name redacted)
Legislative Attorney
[redacted]@crs.loc.gov, 7-....

[87] U.S. Department of Health and Human Services, Office of Inspector General, Nationwide Review of the Centers for Medicate & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight (A-04-07~05064), Oct. 27, 2008, at http://oig.hhs.gov/oas/reports/region4/40705064.pdf.