Reflections on Privacy: Recent Developments in HIPAA Privacy Rule

NUSRAT N. RAHMAN*

ABSTRACT

In 2005, the article "Privacy Year in Review: Developments in HIPAA" discussed the background and motivations behind the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and focused on the Privacy Rule, one of HIPAA's Administrative Simplification provisions. This article updates the (1) the Office for Civil Rights current enforcement of the Privacy Rule and (2) the Department of Justice's current standing regarding prosecution of Privacy Rule violations which were both discussed in the 2005 article. This article also addresses the impact of Hurricane Katrina on the Privacy Rule.

I. INTRODUCTION

In 2005, the article "Privacy Year in Review: Developments in HIPAA"[1] discussed the background and motivations behind the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and focused on one of HIPAA's Administrative Simplification provisions: the Privacy Rule.[2] The article reviewed and analyzed the following four issues: 1) whether the Office of Civil Rights is enforcing the Privacy Rule; 2) whether, in light of *United States v. Gibson*, the Department of Justice is empowered to prosecute individuals as well as covered entities for Privacy Rule violations; 3) the "extent to which the Privacy Rule protects genetic information and its implication for the future of genetic privacy;" and 4) the Privacy Rule's interactions with federal and state laws regarding privacy of health information.[3]

---

* Nusrat N. Rahman is a J.D. candidate at The Ohio State University Moritz College of Law, class of 2007. She received a B.A. in English from University of Rochester. The author would like to thank Professor Peter Swire and Elizabeth Hutton for their assistance and guidance in this article.

[1] Elizabeth Hutton & Devin Barry, *Privacy Year in Review: Developments in HIPAA*, 1 ISJLP 347 (2005) (explains and provides an overview of HIPAA, including the purpose of HIPAA covered entities under HIPAA, identification, and security standards).

[2] *Id*. at 379.

[3] *Id*.

This article updates (1) the Office for Civil Rights current enforcement of the Privacy Rule and (2) the Department of Justice's current standing regarding the prosecution of Privacy Rule violations. Additionally, this article covers new ground on the following issue: the impact of Hurricane Katrina on HIPAA's Privacy Rule.

II. THE PRIVACY RULE

The HIPAA Privacy Rule[4] was issued in accordance with the "Administrative Simplification" provisions of HIPAA. The Administrative Simplification provisions aimed to establish national standards that would "facilitate the electronic exchange of information."[5] A new section entitled "Part C—Administrative Simplification" was added to title XI of the Social Security Act to house the Administrative Simplification provisions.[6] The Administrative Simplification provisions have been codified at 42 U.S.C. §§ 1320d–1320d-8.

Under the Administrative Simplification provisions, Congress provided the Department of Health and Human Services ("HHS") with the authority to promulgate appropriate standards "for transactions, and data elements for such transactions, to enable health information to be exchanged electronically."[7] The Privacy Rule is one of the Administrative Simplification rules established by HHS to ensure "nationwide minimum standards for the protection of what it termed 'individually identifiable health information.'"[8] HHS issued the standards of the Privacy Rule in final form in 2000, and it became effective for health care providers[9] and health plans[10] on April 14,

---

[4] Privacy Rule, 45 C.F.R. § 164 (2005).

[5] Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 642 (2002).

[6] OFFICE OF GENERAL COUNSEL, U.S. DEPARTMENT OF JUSTICE, SCOPE OF CRIMINAL ENFORCEMENT UNDER 42 U.S.C. § 1320d-6 (2005), *available at* http://www.usdoj.gov/olc/hipaa_final.htm.

[7] 42 U.S.C. § 1320d-2 (2005).

[8] Winn, *supra* note 5, at 642.

[9] 45 C.F.R. § 160.103 (2005) ("Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services

2003.[11] The Privacy Rule became effective for small health plans on April 14, 2004.[12]

The Privacy Rule maintains a balance that safeguards individuals' health information, while ensuring that the flow of health information required to provide high quality health care and to protect the public's health, is not compromised.[13] Specifically, the Privacy Rule protects "individually identifiable health information,"[14] which the Privacy Rule refers to as "protected health information (PHI)," "held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral."[15]

A. COVERED ENTITIES UNDER THE PRIVACY RULE

The Privacy Rule applies only to covered entities including: health plans, health care clearinghouses, and any other health care provider "who transmits health information in electronic form in connection with transaction[s]," for which the Secretary of HHS has adopted standards under HIPAA.[16] A fourth group, Medicare prescription drug sponsors, was added as a covered entity by Congress in 2003 as a

---

(as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.").

[10] *Id*. § 160.103 (2005) (defines health plans).

[11] *Id*. § 164.534 (2005).

[12] *Id*.

[13] OFF. OF CIV. RTS, U.S. DEPT. OF HEALTH & HUM. SERVICES, SUMMARY OF THE HIPAA PRIVACY RULE 3 (2003), *available at* http://www.hhs.gov/ocr/privacysummary.pdf.

[14] 45 C.F.R § 160.103 (2005) ("Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.").

[15] OFF. OF CIV. RTS, U.S. DEPT. OF HEALTH & HUM. SERVICES, *supra* note 13, at 5.

[16] 42 U.S.C. § 1320d-1 (2005).

result of the enactment of The Medicare Prescription Drug, Improvement and Modernization Act of 2003. The statute specifically states:

> For purposes of the program under this section, the operations of an endorsed program are covered functions and a prescription drug card sponsor is a covered entity for purposes of applying part C of title XI [42 USCS §§ 1320d et seq.] and all regulatory provisions promulgated thereunder, including regulations (relating to privacy) adopted pursuant to the authority of the Secretary under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note).[17]

Covered entities are generally barred from disclosing PHI for any other purpose other than "treatment, payment, or health care operations."[18]

B. ENFORCEMENT OF THE PRIVACY RULE

Violators of the Privacy Rule are threatened with criminal and civil penalties. The Office for Civil Rights ("OCR"), a division of HHS, investigates and enforces Privacy Rule civil violations. The Department of Justice ("DOJ") enforces criminal violations of the Privacy Rule.

OCR aims for voluntary cooperation by covered entities, and provides technical assistance to covered entities in order to ensure voluntary compliance.[19] The Secretary of HHS is authorized to impose civil penalties for noncompliance with the Privacy Rule. The civil penalties include "$100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000."[20]

---

[17] *Id*. § 1395w-141(h)(6)(A).

[18] 45 C.F.R. § 164.506.

[19] *Id*. § 160.304.

[20] 42 U.S.C. § 1320d-5(a)(1) (2005).

A civil penalty cannot be imposed if: (1) the act "constitutes an offense punishable" by criminal penalties,[21] (2) "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 provision,"[22] or (3) "the failure to comply was due to reasonable cause and not to willful neglect; and the failure to comply is corrected."[23] The Secretary of HHS has discretion to waive the penalty to the extent that "payment of such penalty would be excessive relative to the compliance failure involved."[24]

HHS recently issued its final rules regarding the new comprehensive Enforcement Rule became effective March 16, 2006. The Enforcement Rule unites the process of enforcement for civil violations of all of the HIPAA rules[25] and it establishes uniform guidelines for imposing civil monetary penalties for entities guilty of violating the HIPAA rules.[26]

The Enforcement Rule, however, does not affect enforcement and assessment of criminal violations,[27] this responsibility remains with the DOJ. A criminal violation, which includes a person who makes a "[w]rongful [and knowing] disclosure of individually identifiable health information,"[28] shall

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

---

[21] *Id*. § 1320d-5(b)(1).

[22] *Id*. § 1320d-5(b)(2).

[23] *Id*. § 1320d-5(b)(3)(A).

[24] *Id*. § 1320d-5(b)(4).

[25] HIPAA Administrative Simplification: Enforcement 71 Fed. Reg. 8390, 8391 (Feb 16. 2006) (to be codified at 45 C.F.R. pt. 160 and 164).

[26] Hall, Render, Killian, Heath & Lyman, *HIPAA Enforcement Rule Now in Effect* 1, June 7, 2005, http://www.hallrender.com/library/articles/106/HIPAA%20Enforcement%20Rule%20Now%20In%20Effect.pdf.

[27] *Id*.

[28] 42 U.S.C. § 1320d-6 (2005).

> (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.[29]

III. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS ENFORCEMENT OF THE PRIVACY RULE: MONETARY PENALTIES

HHS is dedicated to a "one voice" approach in enforcing civil violations: "HHS's public health and welfare mission and message must be consistent, and HHS should speak with one voice . . . [B]ecause there is one statutory provision for imposing civil money penalties on covered entities that violate the HIPAA rules, there is one enforcement and compliance policy for the HIPAA rules."[30]

Until the Enforcement Rule went into effect, HHS relied predominately on filed complaints to enforce compliance with HIPAA rules, such as the Privacy Rule.[31] Although HHS also conducted compliance reviews to determine if covered entities were in compliance, it focused mainly on investigating complaints.[32] The Enforcement Rule continues to rely on both filed complaints and compliance reviews to enforce compliance with HIPAA rules.[33]

Under the final section 160.312(a)(1) of the Enforcement Rule, efforts are expended to resolve violations informally.[34] If a matter

---

[29] *Id.* at § 1320d-6(b).

[30] HIPAA Administrative Simplification; Enforcement, 70 Fed. Reg. 20224, 20226 (April 18, 2005) (to be codified at 45 C.F.R. pt. 160 and 164).

[31] *Id*.

[32] *Id.*

[33] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. at 8425.

[34] *Id*.

cannot be resolved in the initial stage of contact or through voluntary compliance then HHS may impose civil money penalties.[35]

To date, no monetary penalties have been imposed. OCR has received over 14,900 complaints as of August 31, 2005.[36] Sixty-eight percent of those complaints have been closed;[37] and two-hundred and thirty-one of the cases have been referred to the Department of Justice for criminal investigation.[38]

Most complaints received by HHS are complaints against individuals rather than covered entities. Civil monetary penalties can only be imposed on covered entities, not individuals. Although the lack of imposition of civil money penalties raises a cautionary flag about the effectiveness of the rule,[39] the manner of civil money penalties may change now that the final Enforcement Rules for civil monetary penalties are effective.[40]

A. HIPAA ENFORCEMENT RULE

The Enforcement Rule which became effective on March 16, 2006, is the final chapter of 42 U.S.C. 1320d-5(a). It adopts a comprehensive and unified approach to enforcing all of the HIPAA Administrative Simplification rules (the Privacy Rule, the Security Rule, the Electronic Transaction and Code Set Rule, and the Identifier Standards).[41]

---

[35] *Id*.

[36] Phoenix Health Systems, *Private Practices & Unauthorized Use of PHI Still Top OCR's 15,000 Privacy Complaints*, HIPAADVISORY.COM, Sept. 27, 2005, http://www.hipaadvisory.com/news/NewsArchives/2005/sep05.htm.

[37] *Id*.

[38] *Id*.

[39] *See* Hutton & Barry, *supra* note 1, for various theories regarding why imposition of monetary penalties has not been forthcoming.

[40] Hutton & Barry, *supra* note 1, at 357.

[41] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. at 8391.

1. VOLUNTARY COMPLIANCE AND USE OF "INFORMAL MEANS" TO ACHIEVE COMPLIANCE

"Encouraging voluntary compliance is the most effective and quickest way of obtaining compliance in most cases."[42] Accordingly, under section 160.304(a) of the Enforcement Rule, the Secretary of HHS seeks and encourages voluntary compliance from covered entities.[43] The Secretary also may "provide technical assistance to covered entities to help them comply voluntarily with the applicable administrative simplification provisions."[44]

Additionally, in accordance with section 160.312 HHS will continue to utilize "informal means" to resolve noncompliance by covered entities,[45] allowing "closure at an early stage to a matter where compliance is in issue and, thus, [obviating] the need to issue a notice of proposed determination."[46]

"Informal means" includes "demonstrated compliance, or a completed corrective action plan or other agreement."[47] The Secretary of HHS has wide discretion to settle any matter of noncompliance and to prompt covered entities to come into compliance voluntarily.[48] The Secretary of HHS also has the authority to settle a case where a civil money penalty has been proposed, or which is in the midst of a hearing.[49]

Although the Enforcement Rule establishes a new unified approach to enforcing all of the HIPAA Administrative Simplification rules, the focus on promoting voluntary compliance and utilizing informal means to resolve noncompliance by covered entities is consistent with HHS past methods.

---

[42] *Id*. at 8394.

[43] *Id*. at 8425.

[44] *Id*. at 8394.

[45] *Id*. at 8425.

[46] *Id*. at 8397.

[47] *Id*. at 8425.

[48] *Id*. at 8400, 8427.

[49] *Id*.

2. STANDARDS FOLLOWED WHEN UNABLE TO ACHIEVE COMPLIANCE THROUGH "INFORMAL MEANS"

If noncompliance is not corrected through "informal means," then HHS must give notice to the covered entity and give the covered entity the opportunity "to submit written evidence of any mitigating factors or affirmative defenses for consideration under sections 160.408 and 160.410 of this part."[50] Affirmative defenses barring imposition of a civil monetary penalty include: (1) an act punishable under the criminal penalty under 42 U.S.C. 1320d-6;[51] (2) establishing to the HHS Secretary's satisfaction that the covered entity "did not have knowledge of the violation . . . and, by exercising reasonable diligence would not have known that the violation occurred;"[52] or (3) the covered entity failed to comply "due to reasonable cause and not willful neglect" and is corrected within

> [t]he 30-day period beginning on the date the covered entity liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred; or . . . [s]uch additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.[53]

While the Secretary must impose monetary penalties where a formal determination is made regarding a violation, the new rule allows for ample opportunities for covered entities to correct their noncompliance prior to the final determination, thus avoiding monetary penalties.[54]

---

[50] HIPAA Administrative Simplification: Enforcement, 70 Fed. Reg. at 20230.

[51] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. at 8427.

[52] *Id*. at 8427.

[53] *Id*.

[54] *Id*. at 8397.

3. CIVIL MONEY PENALTIES FOR VIOLATIONS BY MORE THAN ONE COVERED ENTITY

Section 160.402(b) of the Enforcement Rule requires the HHS Secretary to impose civil monetary penalties on each covered entity if the HHS Secretary finds more than one covered entity violated an administrative simplification provision.[55] If a covered entity, however, "is a member of an affiliated covered entity," then each member is "jointly and severally liable for a civil money penalty . . . unless it is established that another member of the affiliated covered entity was responsible for the violation."[56]

The final section 160.402(b)(2) differs from the proposed rule. Under the proposed rule, even if a covered entity demonstrated that it was not responsible for violating the administrative simplification provision it would still have been liable if another member of the affiliated covered entity was guilty of a violation.[57] The final rule allows an affiliated covered member to avoid liability if it is able to establish that another member was the party responsible for the violation.[58]

Under the final rule, greater protection from liability is afforded to affiliated covered entities. Arguably, the protection is illusive because an affiliated covered entity is protected only when it can identify the member responsible for the violation. The comments of the final rule, however, anticipate that "in most cases, which member was responsible for the violation will be clear—for example, if four of five members of a covered entity distributed privacy notices but the fifth member did not, the violation of the notice distribution requirement of section 164.520 would be attributed to the fifth member."[59] The final

---

[55] HIPAA Administrative Simplification: Enforcement, 70 Fed. Reg. at 20231.

[56] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. at 8427; s*ee also* 45 C.F.R. § 164.105 (2005) for a detailed discussion of what constitutes an affiliated covered entity.

[57] HIPAA Administrative Simplification: Enforcement, 70 Fed. Reg. at 20231-32.

[58] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. at 8401.

[59] *Id*.

rule commentary further asserts that it is unlikely that a situation will arise where the guilty member will not be identified.[60]

Even if a guilty member is not identified, the final rule commentary states that the "inability to assign specific responsibility for a violation to one or more members of an affiliated covered entity should not shield all of its members from liability."[61] Additionally, eliminating joint and several liability may actually result in greater liability for members of an affiliated covered entity: "absent joint and several liability, each member of the affiliated covered entity would be separately liable for the penalty for the violation, e.g., the failure to appoint a privacy officer."[62]

Under no circumstances, however, can more than $25,000 be imposed during a calendar year on all members of an affiliated covered entity that are responsible for identical violations:

> Where responsibility for a violation is allocated to individual covered entities, each covered entity determined to be responsible for the violation would be liable for violations of an identical requirement or prohibition in a calendar year up to the statutory maximum of $ 25,000. If responsibility for particular violations cannot be determined, so that the members of the affiliated covered entity are jointly and severally liable for the violation, the maximum that would be imposed for violations of an identical requirement or prohibition in a calendar year would be $ 25,000.[63]

Thus, the final rule contemplated and considered the opposition faced by the proposed rule: many opposed it on the grounds that "it was unfair to make one covered entity liable for a violation committed by another covered entity."[64] Consequently, the final rule, while relaxing the requirements set forth by the proposed rule, does not

---

[60] *Id*.

[61] *Id*.

[62] *Id*.

[63] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. at 8402.

[64] *Id*. at 8401.

allow for complete evasion of monetary penalties where there is a violation by an affiliated covered entity.

4. VIOLATIONS OF OVERLAPPING PROVISIONS IN A HIPAA RULE

Under section 160.404(b)(2) of the Enforcement Rule, the HHS Secretary can impose only one civil money penalty when the action or omission of a covered entity results in violations of two or more provisions of the same subpart.[65] For example, if a covered entity fails to establish minimum necessary procedures to control use of PHI, and thus violates section 164.514(d)(2) of the Privacy Rule, the covered entity is also in violation of section 164.514(d)(1) of the Privacy Rule, which requires a "minimum necessary standard."[66] The final provision adopted the proposed provision: "treat the act or omission as a violation of only one of the identical administrative simplification provisions, not both, for purposes of imposing civil money penalties."[67]

A covered entity, however, can face separate monetary penalties for violations of different provisions of the same HIPAA rule.[68] For instance, if a covered entity sells its used computers and neglects to scrub the hard drives, which contain protected health information, the covered entity may have violated several separate provisions of a HIPAA rule.[69] In such a case, the covered entity's actions have violated "requirements or prohibitions of different rules promulgated pursuant to different provisions of the statute," and the covered entity can face civil money penalties for each violated provision.[70]

Thus, covered entities will not face multiple civil money penalties when the action or omission of a covered entity results in violations of two or more provisions of the same subpart. As the above example illustrates, however, an action or omission by covered entities can

---

[65] *Id*. at 8427.

[66] HIPAA Administrative Simplification: Enforcement, 70 Fed. Reg. at 20234.

[67] *Id*.

[68] *Id*.

[69] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. at 8404-05.

[70] *Id.*

result in multiple penalties when numerous different provisions of the HIPAA rules are violated. Thus, covered entities should be on alert regarding the consequential violations that may result from their actions or inactions.

5. QUANTIFYING THE NUMBER OF VIOLATIONS

The proposed rule suggested using the following variables to calculate the number of times a covered entity may be responsible for a HIPAA rule violation: "(1) the number of impermissible actions or failures to take required actions; (2) the number of persons involved; and (3) the amount of time during which the violation occurred."[71]

Many comments to the proposed rule "challenged the variable approach of proposed section 160.406 to determining the number of violations."[72] The comments argued that

> the proposed approach was unfair in that it (1) did not allow covered entities to predict the amount of a civil money penalty that would result from a violation, and (2) could maximize the penalty to the statutory cap in virtually any case, which could result in very harsh penalties for relatively minor offenses.
>
> In response, the final rule elected to eliminate the variable approach. Instead, the number of an identical requirement or prohibition (termed "identical violations") will be determined based on the nature of the covered entity's obligation to act or not act under the provision violated, such as its obligation to act in a certain manner, or within a certain time, or with respect to certain persons. With respect to continuing violations, a separate violation will be deemed to occur on each day such a violation continues.[73]

---

[71] HIPAA Administrative Simplification: Enforcement, 70 Fed. Reg. at 20234.

[72] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. at 8405.

[73] *Id*.

Thus, by eliminating the variable approach, the final rule worked to eliminate the concern and confusion that was exhibited in response to the proposed rule. Alternatively, the final rule clearly explains that in determining identical violations, the Secretary will look to the "nature of the obligation" owed by the covered entity "to act (or not act) under the provision violated." Consequently, the final rule exhibits a clearer approach to computing the number of violations.

6. SIX FACTORS CONSIDERED IN DETERMINING CIVIL MONEY PENALTIES

Provision section 160.408 compartmentalizes and provides more detailed guidance in identifying the factors that are considered in determining a HIPAA violation. The Secretary of HHS is to take the following factors into account when determining the amount of civil money penalties.

> (a) The nature of the violation, in light of the purpose of the rule violated.
>
> (b) The circumstances, including the consequences, of the violation, including but not limited to: (1) The time period during which the violation(s) occurred; (2) Whether the violation caused physical harm; (3) Whether the violation hindered or facilitated an individual's ability to obtain health care; and (4) Whether the violation resulted in financial harm.
>
> (c) The degree of culpability of the covered entity, including but not limited to: (1) Whether the violation was intentional; and (2) Whether the violation was beyond the direct control of the covered entity.
>
> (d) Any history of prior compliance with the administrative simplification provisions, including violations, by the covered entity, including but not limited to: (1) Whether the current violation is the same or similar to prior violation(s); (2) Whether and to what extent the covered entity has attempted to correct previous violations; (3) How the covered entity has responded to technical assistance from the

> Secretary provided in the context of a compliance effort; and (4) How the covered entity has responded to prior complaints.
>
> (e) The financial condition of the covered entity, including but not limited to: (1) Whether the covered entity had financial difficulties that affected its ability to comply; (2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity to continue to provide, or to pay for, health care; and (3) The size of the covered entity.
>
> (f) Such other matters as justice may require.[74]

B. CONCLUSION: ENFORCEMENT RULE

Under the new Enforcement Rule, HHS continues to "promote voluntary compliance," and make efforts to use "informal means" to resolve noncompliance. Thus, although covered entities must be aware of the new Enforcement Rule and take appropriate steps to safeguard themselves from violating the new Rule, "there is nothing startling in the rule, nor is it likely to be of substantial concern to most companies, given the limited formal enforcement of HIPAA to date."[75] Alternatively, others anticipate that "[w]ith the framework in place, it's a safe bet that HHS will become more active in its enforcement efforts."[76] Although there are conflicting theories on how the Enforcement Rule will change the climate of enforcement, now that the final rules are in effect, many believe that HHS will pursue HIPAA

---

[74] *Id*. at 8427.

[75] Kirk J. Nahra, *HHS Issues New HIPAA Enforcement Rule,* PRIVACY IN FOCUS, (April 2005), http://www.wrf.com/publication.cfm?publication_id=12085.

[76] Steptoe & Johnson PLLC, Good News! HHS has 'Simplified' HIPAA Enforcement (but not really), 11 WEST VIRGINIA EMPLOYMENT LAW LETTER (M. Lee Smith Publishers LLC, Brentwood, Tenn.), May 2006.

rule violations more aggressively: "the final enforcement rule may have more teeth than some providers may realize."[77]

IV. DEPARTMENT OF JUSTICE'S CURRENT STANDING ON PROSECUTING PRIVACY RULE VIOLATIONS

A. *UNITED STATES V. GIBSON*: THE BEGINNING OF CRIMINAL PROSECUTION

United States v. Gibson marked the first criminal conviction of an individual under the criminal provision of the HIPAA Rule.[78] The DOJ brought charges against Richard Gibson under HIPAA, despite the fact that Gibson was not a covered entity, for wrongfully disclosing individually identifiable health information for personal financial gain.[79] Gibson was sentenced to sixteen months in federal prison.[80]

The decision raised questions regarding who the DOJ can reach in the face of a HIPAA violation. "[T]his decision by the Department of Justice effectively extends the provisions of [T]itle II of HIPAA beyond its primary and secondary targets-covered entities and their "business associates"–to their workforces."[81] Additionally, some warned that the *Gibson* case should serve as an example for covered entities to make reasonable efforts to safeguard individually identifiable health information:

---

[77] Margaret Amatayakul, *HIPAA Enforcement Rule Will More Teeth Equal Bigger Bite? It's No Secret that the Federal Government is Promoting Adoption of Healthcare IT–with Fervor*, HEALTH CARE FIN MGMT., May 2006, at 116.

[78] United States v. Gibson, No. CR04-0374RSM, 2004 WL 2188280 (W.D. Wash. 2004); *See* Hutton & Barry, *supra* note 1, at 359-66 for a more detailed account of the United States v. Gibson case.

[79] Hutton & Barry, *supra* note 1, at 360-61.

[80] Brian D. Annulis, *Identity theft case creates new HIPPA concerns for hospitals. (Health Insurance Portability and Accountability Act)*, 23 HEALTH CARE STRATEGIC MGMT, Jan. 12, 2005, at 11 (2005).

[81] *Id*.

> Gibson is likely to be the first of many criminal prosecutions under HIPAA for the knowing misuse of individually identifiable health information.
>
> It should serve as a reminder to all covered entities that compliance is not a static concept. Covered entities should routinely consider ways to improve their privacy compliance program and initiatives. Is there a way to avoid having people like Gibson work at your institution? If so, what is the cost of implementing that preventative screening measure? How do the costs of implementing that measure compare to the potential benefits?[82]

The heightened concerns raised due to the *Gibson* decision proved to be premature in the wake of the publication of an Office of Legal Counsel Opinion that addressed the issue of who can be liable under the criminal provision 42 U.S.C. § 1320d-6.

B. THE OFFICE OF LEGAL COUNSEL OPINION: CURRENT STATE OF AFFAIRS FOR CRIMINAL ENFORCEMENT OF HIPAA VIOLATIONS

Less than a year after *Gibson*, the DOJ issued a memorandum on June 1, 2005, that appeared to scale back from the extended scope of coverage exhibited by the *Gibson* case. The memorandum was written in response to questions posed by the General Counsel of the Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General, asking for the definition of the scope of criminal enforcement under 42 U.S.C. §1320d-6.[83] Specifically, the DOJ was asked:

> [1] [W]hether the only persons who may be directly liable under section 1320d-6 are those persons to whom the substantive requirements of the subtitle, as set forth in the regulations promulgated thereunder, apply—i.e., health plans, health care clearinghouses, certain health care providers, and Medicare prescription drug card sponsors—or

---

[82] *Id*.

[83] OFFICE OF GENERAL COUNSEL, U.S. DEPARTMENT OF JUSTICE, *supra* note 6.

> whether this provision may also render directly liable other persons, particularly those who obtain protected health information in a manner that causes a person to whom the substantive requirements of the subtitle apply to release information in violation of that law.[84]
>
> [2] [W]hether the "knowingly" element of section 1320d-6 requires only proof of knowledge of the facts that constitute the offense or whether this element also requires proof of knowledge that the conduct was contrary to the statute or regulations.[85]

On the first issue, the OLC opinion concluded only "covered entities" and "those persons rendered accountable by general principles of corporate criminal liability" can be prosecuted for violations under 42 U.S.C. § 1320d-6.[86] Despite the decision in the *Gibson* case, the memorandum was clear that non-covered entities are not directly liable under 42 U.S.C. § 1320d-6: "[o]ther persons may not be liable directly under the provision."[87] The memorandum also pointed out that while the government cannot prosecute violations by non-covered entities under 42 U.S.C. § 1320d-6 directly, such violations "may be prosecuted according to principles either of aiding and abetting liability or of conspiracy liability" pursuant to the federal aiding and abetting statute, 18. U.S.C. § 2 (2000), and the conspiracy statute, 18 U.S.C. §371 (2000).[88]

The second issue addressed what elements are sufficient to meet the "knowing" standard required under 42 U.S.C. §1320d-6. The opinion stated 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."[89] It is the first part of the opinion that has been in the spotlight since the memorandum became public.

---

[84] *Id*.

[85] *Id*.

[86] *Id*.

[87] *Id*.

[88] *Id*.

[89] *Id*.

Peter Swire, C. William O'Neill Professor in Law and Judicial Administration at The Ohio State University Moritz College of Law, who was also the Chief Counselor for Privacy during the Clinton Administration, described the OLC Opinion as being "bad law" and "bad policy."[90] Swire advanced five separate arguments regarding why the OLC opinion is "bad law," reaching the conclusion that from a statutory construction standpoint the OLC opinion reaches an absurd conclusion.[91] For instance, Swire pointed to the fact that a violation of the statute includes the possibility of jail time however, it is impossible for a covered entity to go to jail: "[w]e all know that hospitals and health insurance companies don't go to jail."[92]

From a policy standpoint, Swire fears limiting prosecution of HIPAA violations only against covered entities not only reinforces the political theory that "[i]ndustry pressure has stopped HHS from bringing a single civil case," despite the large number of complaints received, but that "the OLC opinion essentially makes the privacy rule into a voluntary standard."[93] Additionally, Swire notes that the OLC opinion will result in the annulment of Gibson's plea agreement: "[a]lthough it is difficult to guess the exact procedure, it will be difficult to keep him in jail when the Justice Department has announced that the statute does not apply to employees such as he was."[94]

Peter Winn, an Assistant U.S. Attorney in the Western District of Washington offers a different point of view on the OLC Opinion. Winn wrote in an editorial, forthcoming in the ABA Health Lawyer that "Professor Swire's analysis may be unduly pessimistic."[95] Winn noted that although federal prosecutors cannot prosecute anyone other

---

[90] Peter P. Swire, *Justice Department Opinion Undermines Protection of Medical Privacy*, CENTER FOR AMERICAN PROGRESS, June 7, 2005, http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=743281.

[91] *Id.* (all five arguments advanced by Professor Peter Swire).

[92] *Id*.

[93] *Id*.

[94] *Id*.

[95] Peter A. Winn, *Who is Subject to Criminal Prosecution under HIPAA?*, AMERICAN BAR ASSOCIATION (Nov. 4, 2005), *available at* http://www.abanet.org/health/01_interest_groups/01_media/WinnABA_2005-11.pdf (forthcoming in A.B.A. HEALTH LAW.).

than covered entities for HIPAA violations, they can utilize other criminal laws to punish those that violate HIPAA:

> the OLC Opinion . . . leaves open the possibility that employees and business associates could still be prosecuted in other ways, [the OLC Opinion] stating, in particular, that "the liability of persons for conduct that may not be prosecuted directly under section 1320d-6 will be determined by principles of aiding and abetting liability and conspiracy liability."[96]

Winn points out that although on first impression the OLC Opinion seems to limit section 1320d-6 to prosecutions of covered entities, "this holding is limited to *direct* prosecutions only."[97] Winn notes that despite the fact that health care employees and other non-covered entities cannot be prosecuted under section 1320d-6, non-covered entities and individuals can be held responsible for HIPAA violations through other means: "the government can also bring prosecutions under *indirect* liability theories, the scope of criminal liability for the wrongful disclosure of PHI will ultimately be determined by how another criminal statute, 18 U.S.C. § 2(b), interacts with section 1320d-6."[98] Relying on existing case law under 18 U.S.C. § 2(b),[99] Winn concludes that the "prosecutions of employees

---

[96] *Id*.

[97] *Id*.

[98] *Id*.

[99] 18 U.S.C. § 2(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."

In his article, *supra* note 95, Winn also directs attention to the fact that the phrase "or another" was added in 1951 by Congress, three years after the act was originally enacted. Mr. Winn cites to the Senate Report that accompanied the 1951 amendment. Specifically, Mr. Winn cites to the following section of the Senate Report that explains the purpose of the phrase "or another:"

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 of officers and employees of the Government, judges, judicial officers, witnesses, officers or employees or persons connected with national banks or member banks.

and business associates of covered entities appear to remain viable, at least . . . to protect the privacy of patient health information" as contemplated by Congress in enacting Section 1320d-6.[100]

C. DEPARTMENT OF JUSTICE'S RECENT PROSECUTIONS UNDER 42 U.S.C. § 1320d-6: *UNITED STATES V. RAMIREZ*

Peter Winn's prediction, that the OLC opinion will not halt prosecution of individuals for section 1320d-6 violations, found support in a recent case brought against Liz Arlene Ramirez.

An indictment was filed against Ramirez on August 30, 2005, in the United States District Court for the Southern District of Texas, McAllen Division, because she sold the confidential medical record information of an FBI agent to an individual who she thought was working for a drug trafficker.[101]

Ramirez was charged with three counts of wrongful disclosure of individually identifiable health information, pursuant to: 42 U.S.C. §1320d-6(a)(1), 42 U.S.C. § 1320d-6(b)(3), and 18 U.S.C. § 2[102] for the first count; 42 U.S.C. § 1320d-6(a)(2), 42 U.S.C. § 1320d-6(b)(3), and 18 U.S.C. § 2 for the second count; and 42 U.S.C. § 1320d-6(a)(2), 42 U.S.C. § 1320d-6(b)(3), and 18 U.S.C. § 2 for the third

---

Section 2(b) of title 18 is limited by phrase "which if directly performed by him would be an offense against the United States," to persons capable of committing the specific offense…It has been argued that one who is not a bank officer or employee cannot be a principal offender in violation of section 656 or 657 of title 18 and that, therefore, persons not bank officers or employees cannot be prosecuted as principals under section 2(g). Criminal statutes should be definite and certain. 1951 U.S. Code Cong. Serv. 2578, 2583.

[100] Winn, *supra* note 95.

[101] Phoenix Health Systems, *Doctor's Office Employee Convicted of Selling FBI Agent's Medical Records*, HIPAA ADVISORY (Mar. 16, 2006), http://www.hipaadvisory.com/News/newsarchives/2006/mar06.htm.

[102] 18 U.S.C. § 2 reads in the relevant part:

(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.

count.[103] Ramirez faced penalties consisting of fines up to $250,000 and prison terms of up to three years for each separate count.[104]

On March 6, 2006, at a hearing before U.S. District Judge Randy Crane, Ramirez pled guilty to the "federal felony offense of wrongfully using a unique health identifier with the intent to sell individually identifiable health information for personal gain."[105] On March 16, 2006, Attorney Chuck Rosenberg announced Ramirez's conviction and noted that "Ramirez faces a maximum punishment of ten (10) years in federal prison, without parole, and a $250,000 fine at her sentencing set for June 8, 2006."[106]

The outcome of *Ramirez* demonstrates that the OLC opinion has not halted prosecution of individuals under Section 1320d-6.

V. HIPAA PRIVACY RULE IN THE FACE OF NATURAL CATASTROPHES SUCH AS HURRICANE KATRINA

Hurricane Katrina has been described as one of the "biggest disaster[s] in U.S. history."[107] The aftermath of Hurricane Katrina included thousands of displaced Mississippi and New Orleans residents, many of whom were uncertain about where their family members were, and many in need of health care.[108] In response, on September 4, 2005, the Secretary of Health and Human Services, Michael O. Leavitt, declared "a federal public health emergency" for Louisiana, Alabama, Mississippi, Florida, and Texas.[109] Pursuant to

---

[103] United States v. Liz Arlene Ramirez, Warrant, Criminal No. M-05-708, McAllen Division.

[104] *Id*.

[105] Phoenix Health Systems, *supra* note 101.

[106] *Id*.

[107] Amanda Ripley, *How Did This Happen?*, TIME, Sept. 12, 2005, at 52.

[108] Stacey A. Tovino, *Hurricane Katrina and the HIPAA Privacy Rule* 1, HEALTH LAW AND POLICY INSTITUTE (Sept. 2005), *available at* http://www.law.uh.edu/healthlaw/perspectives/September2005/(ST)Katrina.pdf.

[109] Gina Marie Stevens, CONG. RES. SERV., Hurricane Katrina: HIPAA Privacy and Electronic Health Records of Evacuees (Oct. 28, 2005), *available at* http://digital.library.unt.edu/govdocs/crs//data/2005/upl-meta-crs-7766/RS22310_2005Oct28.pdf.

Section 1135 of the Social Security Act,[110] Secretary Leavitt suspended certain requirements under HIPAA, among other health care laws, to facilitate care for individuals in need of health care in affected areas.[111] Specifically, Secretary Leavitt waived the following provisions for the state of Florida, Alabama, Louisiana, Mississippi, and Texas, which mandate penalties and sanctions for non-compliance by covered entities.

> (i) [T]he requirements to obtain a patient's oral agreement to speak with family members or friends, or orally opt out of the facility directory under 45 C.F.R. §§ 164.510; (ii) the requirement to distribute a notice of privacy practices under 45 C.R.F. §§ 164.520; and (iii) a patient's right to request privacy restrictions or confidential communications under 45 C.F.R. §§ 164.522 . . . The effective period of the waivers is for a period of time not to exceed 72 hours from implementation of a hospital's disaster protocol.[112]

Additionally, section 1176(b) of the Social Security Act provides that "HHS may not impose a civil money penalty where the failure to comply is based on reasonable cause and is not due to willful neglect, and the failure to comply is cured within a 30-day period."[113] In response to Katrina, HHS allowed for extended periods of time to cure noncompliance with the Privacy Rule and took into consideration the surrounding circumstances for noncompliance:

> OCR [the Office for Civil Rights at HHS] will not take enforcement action or seek to impose civil money penalties where, due to the urgency of the circumstances arising from Hurricane Katrina, a covered entity, its business associates or their agents, are unable to formalize such agreements as required by the Rule in sufficient time to meet the immediate

---

[110] Vinson & Elkins L.L.P., Health Care Special Alert, Health Law Issues Raised by Hurricane Katrina (2005) *available at* http://www.velaw.com/pdf/resources/hh090605.pdf.

[111] *Id*.

[112] *Id.*

[113] *Id*.

> needs of the evacuees, but appropriately execute the required agreements as soon as practicable.[114]

OCR also issued two separate Special Bulletins in response to Hurricane Katrina. The first bulletin was issued on September 2, 2005,[115] and the second bulletin was issued on September 9, 2005.[116] The guidelines set forth in the Special Bulletins are applicable to all providers covered under HIPAA.

A. OCR FIRST SPECIAL BULLETIN: PERMITTED DISCLOSURES

The first bulletin emphasized the range of disclosures permitted by covered entities in response to natural catastrophes such as Hurricane Katrina: "HIPAA Privacy Rule allows patient information to be shared to assist in disaster relief efforts, and to assist patients in receiving the care they need."[117] The bulletin provided information in the following four areas:

> 1. *Treatment*. Health care providers are authorized to disclose health information if necessary to provide treatment. Health care providers are also permitted to disclose patient information if it is required for payment purposes.[118]
>
> 2. *Notification*. Health care providers are authorized to disclose patient information to the extent necessary

---

[114] Bulletin from OFF. OF CIV. RTS, U.S. DEPT. OF HEALTH & HUM. SERVICES, Hurricane Katrina Bulletin #2: HIPAA Privacy Rule Compliance Guidance and Enforcement Statement for Activities in Response to Hurricane Katrina 2 (Sept. 9, 2005), *available at* http://www.hhs.gov/ocr/hipaa/EnforcementStatement.pdf [hereinafter Bulletin #2].

[115] Bulletin from OFF. OF CIV. RTS, U.S. DEPT. OF HEALTH & HUM. SERVICES, Hurricane Katrina Bulletin: HIPAA Privacy and Disclosures in Emergency Situations (Sept. 2, 2005), *available at* http://privacyruleandresearch.nih.gov/pdf/HurricaneKatrina.pdf [hereinafter Bulletin #1].

[116] Bulletin #2, *supra* note 114.

[117] Bulletin #1, *supra* note 115, at 1.

[118] *Id*.; *See also* 45 C.F.R.§ 164.501 (defines treatment).

to "identify, locate, and notify family members, guardians, or anyone else responsible for the individual's care of the individual's location, general condition, or death."[119] The bulletin guides health care providers to get "verbal permission from individuals, when possible," however, when verbal permission is not possible the providers may "share information for these purposes if, in their professional judgment, doing so is in the patient's best interest."[120] Thus, in circumstances involving catastrophes such as Katrina, sharing of patient information to the authorities, press, or public at large is permitted even in the absence of permission by individuals. Additionally, health care providers are not required to obtain patient permission to disclose information to disaster relief organizations such as the American Red Cross "if doing so would interfere with the organization's ability to respond to the emergency."[121]

3. *Imminent Danger*. Health care providers are free to disclose patient information to the extent "necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public."[122] Of course, the disclosure must be made in good faith, only to the extent necessary, and in compliance "with applicable law and the provider's standards of ethical conduct."[123]

4. *Facility Directory*. When patient inquiries are made by individuals to health care facilities who maintain

---

[119] Bulletin #1, *supra* note 115, at 1.

[120] *Id.*

[121] *Id*. at 2; *see* 45 C.F.R. § 164.510(b)(4).

[122] Bulletin #1, *supra* note 115, at 2.

[123] *Id*.; *see* 45 C.F.R. § 164.512(j)(1) (2005).

> a directory of patients, the health care facilities are authorized to disclose patient information regarding patients' locations in the facility, and the general health conditions of patients.[124]

Generally, under 45 C.F.R. § 164.510 covered entities cannot disclose protected health information unless the individual "is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section."[125] Additionally, under 45 C.F.R. § 164.510 "[t]he covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section."[126] In response to Hurricane Katrina, however, the federal privacy regulations of 45 C.F.R. §164.510 were relaxed.

B. OCR SECOND SPECIAL BULLETIN

The second OCR Special Bulletin, "HIPAA Privacy Rule Compliance Guidance and Enforcement Statement for Activities in Response to Hurricane Katrina," expanded on the first OCR Special Bulletin's message, that a broad range of uses are authorized for emergency situations under the HIPAA Privacy Rule.[127] The second bulletin permits "business associates that are managing such information on behalf of covered entities may make these disclosures to the extent permitted by their business associate agreement with the covered entities, as provided in the Privacy Rule."[128] Additionally, covered entities and business associates are authorized to disclose patient information on evacuees to third parties "for that party to manage the health information and share it as needed for providing

---

[124] Bulletin #1, *supra* note 115, at 2; *see* 45 C.F.R. § 164.510 (i)(B).

[125] 45 C.F.R. § 164.510 (2006).

[126] *Id*.

[127] Bulletin #2, *supra* note 114, at 1.

[128] *Id*.

health care to the evacuees."[129] Of course, proper safeguards need to be in place to ensure health information being exchanged is protected in accordance with the Privacy Rule.[130]

C. HEALTH CARE INFORMATION SHARING HITS CYBERSPACE: KATRINAHEALTH.ORG

KatrinaHealth.org, an online Electronic Health Record ("HER") system, was launched by the government soon after Hurricane Katrina.[131] This program allows authorized pharmacists and doctors to gain access to Katrina evacuees' prescription drug information, in order to renew prescriptions, coordinate health care efforts, and avoid prescribing medication that can lead to adverse reactions.[132] Additionally, authorized pharmacists and doctors can also inquire into patients' allergy information, "clinical pharmacology drug information," and view "therapeutic duplication reports and alerts."[133] This information is accessible from anywhere in the country by licensed doctors and pharmacists treating Katrina evacuees.[134] The launch and operation of KatrinaHealth.org was accomplished through the help "of federal, state, and local governments" and "is being operated by a national foundation, several private businesses, and national organizations of physicians and other health professionals."[135]

At the time of its launch, KatrinaHealth.org had drug records of over 800,000 individuals and contained records from 150 zip codes of areas affected by Katrina.[136] The personal prescription information was compiled and made available by: "private companies; pharmacy benefit managers; chain pharmacies; local, state, and federal agencies;

---

[129] *Id.* at 2.

[130] *Id*.

[131] Stevens, *supra* note 109, at 1.

[132] KatrinaHealth, http://www.katrinahealth.org/ (last visited Nov. 27, 2005).

[133] Stevens, *supra* note 109, at 5.

[134] *Id*.

[135] KatrinaHealth, *supra* note 132.

[136] Stevens, *supra* note 109, at 4.

and a national foundation."[137] These entities relied on a "variety of government and commercial sources," including over 150 private and public electronic databases maintained by organizations including Blue Cross and Blue Shield Association and Medicaid, to garner evacuees' prescription information.[138]

Measures have been taken to ensure appropriate safeguards are in place so patients' privacy is not being violated. There are tools in place to prevent unauthorized access. For instance, the site has "read only" access.[139] Additionally, doctors have to be "authenticated by the American Medical Association, which houses a master list of U.S. certified physicians," before they can utilize the online program.[140] The National Community Pharmacists Association ("NCPA") is similarly responsible for authenticating pharmacists before permitting them access to prescription records.[141] Medication information involving "certain sensitive healthcare conditions (HIV/AIDS, mental health issues, and substance abuse or chemical dependencies)" is not available through the site.[142]

The developers of the program have also noted that security and privacy was a focal point in designing KatrinaHealth.org.[143] Zoe Baird, president of the Markle Foundation, one of the organizations responsible for providing funding and knowledge to the effort, has stated: "[p]rivacy, security and ease-of-use were central to the design."[144] David J. Brailer, national coordinator for health information technology at HHS, also commented on the involvement

---

[137] *Id*.

[138] *Id*.

[139] Danielle Belopotosky, *HEALTH: Medical Web Site Aids Hurricane Victims, Doctors*, NAT'L J. TECH. DAILY, Sept. 22, 2005, at PM Edition.

[140] *Id*.

[141] Stevens, *supra* note 109, at 5.

[142] *Id*.

[143] *Id*.

[144] Belopotsky, *supra* note 139, at PM Edition.

of the Centers for Disease Control and the HHS Office for Civil Rights to ensure protection of privacy concerns.[145]

Thus, although a large amount of health information is now readily available to certain authorized individuals, the safeguards in place are designed to prevent misuse of the information.

D. CONCLUSION: HIPAA PRIVACY RULE IN LIGHT OF HURRICANE KATRINA

The HIPAA Privacy Rule appears to be flexible in times of national emergency. The Special Bulletins in response to Katrina and the implementation of KatrinaHealth.org emphasizes HIPAA Privacy Rule's permissibility of disclosure of protected health information in emergency situations. Covered entities, however, must disclose health information protected by the Privacy Rule in good faith, and only to the extent necessary under the circumstances.

VI. CONCLUSION

Within the last year new questions and issues have arisen pertaining to the Privacy Rule. One issue that has remained the same, however, is the concern over OCR's failure to enforce civil monetary penalties for complaints regarding HIPAA violations. The number of complaints received by OCR regarding civil violations has continued to grow, yet no civil monetary penalties have been enforced by OCR to date. However, now that the final rules of the Enforcement Rule are effective, a different climate for enforcement of civil monetary penalties has arisen. Time will expose the impact the Enforcement Rule will have in enforcing civil monetary penalties.

The DOJ's standing in prosecuting Privacy Rule violations in light of *United States v. Gibson* and the OLC Opinion also raised concerns regarding enforcement of the Privacy Rule. Some feared that the OLC Opinion scaled back from the extended scope of coverage exhibited by the *Gibson* case. The outcome in *United States v. Ramirez*, however, affirms that the OLC opinion did not deplete the DOJ of its ability to prosecute individuals for Privacy Rule violations.

The tragedy of Hurricane Katrina raised the important question of how the Privacy Rule reacts and adjusts to situations of national

---

[145] *Id*.

emergency. The issuance of the two Special Bulletins by OCR, the formation of KatrinaHealth.org, and steps taken by Secretary of HHS, Michael O. Leavitt, to suspend certain requirements under HIPAA, established that the Privacy Rule can be flexible in times of national emergency, and under such circumstances the Privacy Rule allows for disclosure of protected health information if it is necessary to facilitate care for those in need.