Order Code RS21505
April 24, 2003

Compliance with the HIPAA Medical Privacy Rule

Gina Marie Stevens
Legislative Attorney
American Law Division

Summary

As of April 14, 2003, most health care providers (including doctors and hospitals) and health plans are required to comply with the new Privacy Rule mandated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and must comply with national standards to protect individually identifiable health information. The HIPAA Privacy Rule creates a federal floor of privacy protections for individually identifiable health information; establishes a set of basic consumer protections; institutes a series of regulatory permissions for uses and disclosures of protected health information; permits any person to file an administrative complaint for violations; and authorizes the imposition of civil or criminal penalties. In hearings prior to the effective date of the Rule, there was widespread concern over aspects of the rule, including the extent to which it preempted state laws. On April 17, 2003, HHS published an interim final rule establishing the rules of procedure for investigations and the imposition of civil money penalties concerning violations. This interim final rule will be effective May 19, 2003 through September 16, 2003. HHS plans to issue a complete Enforcement Rule with both procedural and substantive provisions after notice-and-comment rulemaking. This report will be updated.

Background. In order to "improve portability and continuity of health insurance coverage in the group and individual markets,"[1] Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA) on August 21, 1996, P. L. 104-191, 110 Stat. 1936, 42 U.S.C. §§ 1320d *et seq.* Subtitle F of Title II of HIPAA is entitled "Administrative Simplification," and states that the purpose of the subtitle is to improve health care by "encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[2] Sections 261 through 264 of HIPAA contain the administrative

[1] H.R. Rep. No. 104-496, at 1, 66-67, reprinted in 1996 U.S.C.C.A.N. 1865, 1865-66.

[2] 110 Stat. 2021.

simplification provisions.[3] HIPAA requires health care payers and providers who transmit transactions electronically to use standardized data elements to conduct financial and administrative transactions. Section 262 directs HHS to issue standards to facilitate the electronic exchange of information.[4] Section 263 of HIPAA delineates the duties of the National Committee on Vital and Health Statistics. Section 264 of HIPAA requires HHS to submit to the Congress detailed recommendations on standards with respect to privacy rights for individually identifiable health information. In the absence of the enactment of federal legislation, HIPAA required HHS to issue privacy regulations. The final Privacy Rule was issued by HHS and published in the *Federal Register* on December 28, 2000 at 65 Fed. Reg. 82462, shortly before the Clinton Administration left office. The Privacy Rule went into effect on April 14, 2001. On August 14, 2002, HHS published in the *Federal Register* a modified Privacy Rule, 67 Fed. Reg. 53181.[5] Enforcement of the Privacy Rule began on April 14, 2003, except for small health plans (those with annual receipts of $5 million or less) who have until April 2004 to comply.

The HIPAA Privacy Rule covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically.[6] Covered entities are bound by the new privacy standards even if they contract with others (called "business associates") to perform essential functions. HIPAA does not give HHS authority to regulate other private businesses or public agencies. Covered entities that fail to comply with the rule are subject to civil and criminal penalties,[7] but individuals do not have the right to sue for violations of the rule. Instead, the law provides that individuals must direct their complaints to HHS' Office for Civil Rights (OCR).[8] OCR maintains a Web site with information on the new regulation, including guidance at [http://www.hhs.gov/ocr/hipaa/]. HHS also recently issued a 20 page "Summary of the HIPAA Privacy Rule."[9] HHS will enforce the civil money penalties, and the Department of Justice will enforce the criminal penalties. Criminal penalties may be imposed if the offense is committed under false pretenses, with intent to sell the information or reap other personal gain.

HIPAA authorizes the HHS Secretary to impose civil money penalties of up to $25,000 for each year for those entities failing to comply with the privacy rule.[10] Several statutory limitations are imposed on the Secretary's authority to impose civil money penalties (CMP). A penalty may not be imposed: with respect to an act that constitutes an offense punishable under the criminal penalty provision; "if it is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by

---

[3] See CRS Report RS20934, *A Brief Summary of the Medical Privacy Rule*.

[4] HHS has issued final regulations on standards for security, transactions and code sets, employer identifiers, and privacy. See [http://www.hhs.gov/news/press/2002pres/hipaa.html].

[5] [http://www.hhs.gov/ocr/hipaa/finalreg.html].

[6] For information on covered entities, see [http://www.cms.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp].

[7] 65 Fed. Reg. 82,462, 82,487 (Dec. 28, 2000); see [http://www.hhs.gov/ocr/hipaa/finalreg.html].

[8] See [http://www.ehcca.com/presentations/hipaa6/campanelli.pdf].

[9] [http://www.hhs.gov/ocr/privacysummary.pdf].

[10] 42 U.S.C. § 1320d-5(a)(1).

exercising reasonable diligence would not have known, that such person violated the provisions;"[11] if "the failure to comply was due to reasonable cause and not to willful neglect" and is corrected within a certain time period.[12] A CMP may be reduced or waived "to the extent that the payment of such penalty would be excessive relative to the compliance failure involved."[13] In addition, a number of procedural requirements are incorporated by reference in HIPAA that are relevant to the imposition of CMP's.[14] The Secretary may not initiate a CMP action "later than six months after the date" of the occurrence that forms the basis for the CMP action. The Secretary may initiate a CMP by serving notice in a manner authorized by Rule 4 of the Federal Rules of Civil Procedure. The Secretary must give written notice to the person to 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."[15] Judicial review of the Secretary's determination and the issuance and enforcement of subpoenas is available in the United States Court of Appeals.

With respect to ascertaining compliance with and enforcement of the Privacy Rule, the Secretary of HHS is to seek the voluntary cooperation of covered entities. The Secretary is authorized to provide technical assistance to covered entities in order to facilitate their voluntary compliance. 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; investigating complaints and conducting compliance reviews; and seeking civil monetary penalties and making referrals for criminal prosecution.

An individual may file a compliant with the Secretary if the individual believes that the covered entity is not complying with the rule.[16] Complaints must be filed in writing, either on paper or electronically; name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of the Privacy Rule; and be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless the time limit is waived by the Secretary for good cause shown. Complaints to the Secretary may be filed only with respect to alleged violations occurring on or after April 14, 2003. 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.[17] Individuals may file written complaints with OCR by mail, fax or e-mail. For information about the Privacy Rule or the process for filing a complaint with OCR, they may contact any OCR office or go to [http://www.hhs.gov/ocr/howtofileprivacy.htm]. After April 14, 2003, individuals have

---

[11] 42 U.S.C. § 1320d-5(b)(2).

[12] 42 U.S.C. § 1320d-5(b)(3).

[13] 42 U.S.C. § 1320d-5(b)(4).

[14] 42 U.S.C. § 1320d-5(a)(2).

[15] 42 U.S.C. § 1320a-7a(c)(2).

[16] 45 CFR section 160.306.

[17] 65 Fed. Reg. At 82,474, 82,487.

a right to file a complaint directly with the covered entity, and are directed to refer to the covered entity's notice of privacy practices for information about how to file a complaint.

The Secretary's investigation may include a review of the policies, procedures, or practices of the covered entity, and of the circumstances regarding the alleged acts or omissions. The Secretary is also authorized to conduct compliance reviews. 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. 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. If the Secretary determines that the matter cannot be resolved informally, the Secretary may issue written findings documenting the noncompliance. In cases where no violation is found, the Secretary is to inform the covered entity and the complainant in writing.

On April 17, 2003 HHS published an interim final "Enforcement Rule" that applies to standards, including the Privacy Rule, adopted under the Administrative Simplification provisions of HIPAA, 68 *Fed. Reg.* 18895.[18] The interim final rule establishes procedures for investigations, imposition of penalties, and hearings for civil money penalties; and is effective May 19, 2003 thru September 16, 2003. It is to be revised when HHS issues a complete Enforcement rule that will include procedural **and** substantive requirements for the imposition of civil money penalties, such as HHS' policies for determining violations and calculating CMP's. Although HHS recognized that the Administrative Procedure Act (APA) requires that most of the provisions of the complete Enforcement Rule be promulgated through notice-and-comment rulemaking, it concluded that the interim final rule's procedural provisions are exempted from the requirement for notice and comment rulemaking under the "rules of agency . . . procedure, or practice" exemption of the APA, 5 U.S.C. § 553(b)(3)(A). As a result, HHS published the procedural rules in final form without notice-and-comment to inform covered entities and the public of the procedural requirements for compliance. In addition, HHS requests public comment thru June 16, 2003 on the interim final rule.

The National Committee on Vital and Health Statistics (NCVHS) serves as the statutory public advisory body to the Secretary of Health and Human Services in the area of health data and statistics.[19] As part of its responsibilities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the National Committee on Vital and Health Statistics (NCVHS) monitors the implementation of the Administrative Simplification provisions of HIPAA, including the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule). Last fall, the NCVHS held three hearings to learn about the implementation activities of covered entities. In its November 2002 letter to Secretary Thompson summarizing its findings the Committee stated that "there is an extremely high level of confusion, misunderstanding, frustration, anxiety, fear, and

---

[18] Department of Health and Human Services, Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings, 68 Fed. Reg. 18895 (Apr. 17, 2003), at [http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-9497.pdf].

[19] 42 U.S.C. 242k(k).

anger as the April 14, 2003 compliance date nears."[20] Reportedly the Privacy Rule has "touched off a quiet revolution in the health care industry."[21] According to NCVHS, the OCR is widely viewed as not providing adequate guidance and technical assistance as evidenced by the lack of model notices of privacy practices, acknowledgments, authorizations, and other forms. The general guidance was judged to be of limited value because of special industry or professional circumstances, and NCVHS reported that witnesses conveyed a great sense of frustration that they could not obtain clarification from OCR or answers to the questions they submitted. Covered entities report the undertaking of substantial compliance measures ranging from the adoption of new policies, the training of employees, and the development of privacy notices.

Another area of widespread concern at the NCVHS hearings was HIPAA preemption. According to NCVHS, witnesses said that issues of preemption made compliance much more difficult, costly, and complicated. The term "preemption" is a judicial doctrine that originated through interpretation of the Supremacy Clause of the United States Constitution.[22] In effect, the Supremacy Clause stands for the proposition that the Constitution and the laws of the federal government rise above the laws of the states. As a result, federal law will always override state law in cases of conflict. Absent a direct conflict, however, preemption depends on the intent of Congress. Such intent may be express or implied. Express preemption exists when Congress explicitly commands that a state law be displaced. Where Congress has not expressly preempted state and local laws, two types of implied federal preemption may be found: field preemption, in which federal regulation is so pervasive that one can reasonably infer that states or localities have no role to play, and conflict preemption, in which "compliance with both federal and state regulations is a physical impossibility, or where the state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[23]

HIPAA sets forth a general rule, based on the principles of conflict preemption. Basically, this rule establishes that any federal regulation resulting from implementation of the Act preempts any contrary state law.[24] "Contrary" is defined as situations where: (1) a covered entity would find it impossible to comply with both the state and the federal requirements, or (2) when the state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.[25] Congress established three exceptions to this general rule. First, there is an exception for state laws that the Secretary

---

[20] [http://ncvhs.hhs.gov/021125lt.htm].

[21] Robert Pear, *Health System Wearily Prepares for Privacy Rule*, N.Y. TIMES, Apr. 6, 2003; [http://query.nytimes.com/gst/abstract.html?res=F40C13FD395C0C758CDDAD0894DB404482]

[22] The Supremacy Clause provides:

"This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any state to the Contrary notwithstanding." U.S.Const. art. VI, cl. 2.

[23] *Gade v. National Solid Wastes Mgmt. Assn.*, 505 U.S. 88, 98 (1992).

[24] 42 U.S.C. § 1320d-7(a)(1).

[25] 45 C.F.R. 160.202.

determines are necessary to prevent fraud and abuse, to ensure appropriate state regulation of insurance and health plans, for state reporting on health care delivery, or for other purposes.[26] The second exception provides that state laws will not be superseded if the Secretary determines that the law addresses controlled substances.[27] Both of these exceptions require an affirmative "exception determination" from the Secretary of HHS for the state law not to be preempted.[28] The third exception provides that state laws will not be preempted if they relate to the privacy of individually identifiable health information and are "more stringent" than the federal requirements.[29] A state law is "more stringent" if it meets one or more of the following criteria: 1) the state law prohibits or further limits the use or disclosure of protected health information, except if the disclosure is required by HHS to determine a covered entity's compliance or is to the individual who is the subject of the individually identifiable information; 2) the state law permits individuals with greater rights of access to or amendment of their individually identifiable health information; provided, however, HIPAA will not preempt a state law to the extent that it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian or person acting in loco parentis of such minor; 3) the state law provides for more information to be disseminated to the individual regarding use and disclosure of their protected health information and rights and remedies; 4) the state law narrows the scope or duration of authorization or consent, increases the privacy protections surrounding authorization and consent, or reduces the coercive effect of the surrounding circumstances; 5) the state law imposes stricter standards for record keeping or accounting of disclosures; 6) the state law strengthens privacy protections for individuals with respect to any other matter.[30]

In addition to the general rule and exceptions, Congress "carved out" two provisions whereby certain areas of state authority will not be limited or invalidated by HIPAA rules. First, the public health "carve out" saves any law providing for the reporting of disease or injury, child abuse, birth, or death for the conduct of public surveillance, investigation or intervention.[31] The second "carve out" allows states to regulate health plans by requiring the plans to report, or provide access to, information for the purpose of audits, program monitoring and evaluation, or the licensure or certification.[32]

Legislation. S. 16, The Equal Rights and Equal Dignity for Americans Act of 2003, would, in section 903, reverse the August 2002 modifications to the privacy rule.

---

[26] 42 U.S.C. § 1320d-7(a)(2)(A)(i).

[27] 42 U.S.C. § 1320d-7(a)(2)(A)(ii).

[28] See 45 C.F.R. 160.203(a), 160.204.

[29] 42 U.S.C. § 1320d-7(a)(2)(B) in conjunction with 42 U.S.C. 1320d-2 note (Section 264(c)(2) of Public Law 104-191).

[30] See 45 C.F.R. 160.202.

[31] 42 U.S.C. 1320d-7(b).

[32] 42 U.S.C. 1320d-7(c).