

Statutory Background

HIPAA became law in 1996 (Public Law 104-191). Subtitle F of Title II of HIPAA, entitled "Administrative Simplification," requires the Secretary of HHS to adopt national standards for certain information-related activities of the health care industry. The purpose of subtitle F is to improve the Medicare program under title XVIII of the Social Security Act ("Act"), the Medicaid program under title XIX of the Act, and the efficiency and effectiveness of the health care system, by mandating the development of standards and requirements to enable the electronic exchange of certain health information. Section 262 of subtitle F added a new Part C to Title XI of the Act. Part C (42 U.S.C. 1320d-1320d-8) requires the Secretary to adopt national standards for certain financial and administrative transactions and various data elements to be used in those transactions, such as code sets and certain unique health identifiers. Recognizing that the industry trend toward computerizing health information, which HIPAA encourages, may increase the access to that information, the statute also requires national standards to protect the security and privacy of the information.

The HIPAA provisions, by statute, apply only 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.

42 U.S.C. 1320d-1(a)

Collectively, these entities are known as "covered entities." The statute requires certain consultations with industry as a predicate to the issuance of standards and gives most covered entities 2 years (small health plans have 3 years) to come into compliance with the standards, once adopted. 42 U.S.C. 1320d-1(c), 42 U.S.C. 1320d-4(b). The statute establishes civil money penalties and criminal penalties for violations. 42 U.S.C. 1320d-5, 42 U.S.C. 1320d-6. HHS will enforce the civil money penalties, while the U.S. Department of Justice will enforce the criminal penalties.

HIPAA's civil money penalty ("CMP") provision authorizes the Secretary to impose CMPs, as follows:

- (1) *In general.* Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part [42 U.S.C. 1320d *et seq.*] a penalty of not more than \$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.

(2) *Procedures.* The provisions of section 1128A [42 U.S.C. 1320a-7a] (other than subsections (a) and (b) and the second sentence of subsection (f)) shall apply to the imposition of a civil money penalty under this subsection in the same manner as such provisions apply to the imposition of a penalty under such section 1128A.

42 U.S.C. 1320d-5(a)

Subsection (b) of section 1320d-5 sets out a number of substantive limitations on the Secretary's authority to impose CMPs. First, a CMP may not be imposed with respect to an act that "constitutes an offense punishable" under the criminal penalty provision. 42 U.S.C. 1320d-5(b)(1). Second, a CMP may not be imposed "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 provision." 42 U.S.C. 1320d-5(b)(2). Third, a CMP may not be imposed if the failure to comply was due "to reasonable cause and not to willful neglect" and is corrected within a certain time. 42 U.S.C. 1320d-5(b)(3). Finally, a CMP may be reduced, if not waived entirely, "to the extent that the payment of such penalty would be excessive relative to the compliance failure involved." 42 U.S.C. 1320d-5(b)(4).

As noted above, HIPAA incorporates by reference certain provisions of section 1128A of the Act (42 U.S.C. 1320a-7a). Those provisions, as relevant here, provide a number of procedural requirements with respect to the imposition of CMPs. 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. The Secretary may initiate a CMP action by serving notice "in any manner authorized by Rule 4 of the Federal Rules of Civil Procedure." 42 U.S.C. 1320a-7a(c)(1). A person upon whom the Secretary seeks to impose a CMP must be given written notice and an opportunity for a determination to be 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." 42 U.S.C. 1320a-7a(c)(2). There are provisions authorizing the sanctions the hearing officer may impose for misconduct in connection with the CMP proceeding, judicial review of the Secretary's determination in the United States Court of Appeals for the circuit in which the person resides, and the

issuance of subpoenas by the Secretary and the enforcement of those subpoenas. 42 U.S.C. 1320a-7a(c)(4), (e), (j). These provisions are discussed more fully below.

Regulatory Background

As noted above, HIPAA requires the Secretary of HHS to adopt a number of national standards to facilitate the exchange of certain health information. The Secretary has already issued a number of these HIPAA standards by regulation. We summarize these HIPAA Administrative Simplification rules below.

- Regulations implementing the statutory requirement for the adoption of standards for transactions and code sets ("Transactions Rule") were published on August 17, 2000 (65 FR 50312), and were recently modified (68 FR 8381, February 20, 2003). The Transactions Rule became effective on October 16, 2000, with an initial compliance date of October 16, 2002 for covered entities other than small health plans. The passage of the Administrative Simplification Compliance Act, Pub. L. 107-105, in 2001 enabled covered entities to obtain an extension of the compliance date to October 16, 2003 by filing a compliance plan by October 15, 2002. If a covered entity (other than a small health plan) did not file such a plan, it was required to comply with the Transactions Rule by October 16, 2002. All covered entities must be in compliance with the Transactions Rule, as modified, by October 16, 2003.

- Regulations implementing the statutory requirement for the adoption of privacy standards were published on December 28, 2000 (65 FR 82462) ("Privacy Rule"). The Privacy Rule became effective on April 14, 2001, with an initial compliance date of April 14, 2003 for covered entities other than small health plans. Modifications to the Privacy Rule were published on August 14, 2002 (67 FR 53182), and compliance with the modified privacy standards is required by the initial compliance date, April 14, 2003, for those covered entities that must comply by that date.

- Regulations implementing the statutory requirement for the adoption of an employer identifier standard were published on May 31, 2002 (67 FR 38009) and became effective on July 30, 2002. The initial compliance date is July 30, 2004 for most covered entities; small health plans have until July 30, 2005 to come into compliance.

- Regulations implementing the statutory requirement for the adoption of security standards were published on February 20, 2003 (68 FR 8334). They