A HIPAA PRIMER

By Michael W. Drumke

The Health Insurance Portability and Accountability Act of 1996[1] (HIPAA) established new regulations for the health care industry and created a national framework for privacy protection, thereby changing the treatment of personal medical information. In the years preceding the implementation of HIPAA, newly elected President William J. Clinton pursued legislation to provide universal health care coverage to all Americans.[2] With critics of the Clinton administration's plan prevailing, Congress subsequently enacted HIPAA through amendments to the Internal Revenue Code of 1986 and the addition of Part C to Title XI of the Social Security Act, 42 U.S.C. §§ 1320d *et seq.*[3] According to the preamble, HIPAA was introduced "to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."[4]

During the legislative process, observers expressed concerns that the proposed increased use of information technology would endanger the ability to protect health information; hence, Congress added certain privacy and security rules.[5] Prior to the promulgation of HIPAA, state common law and limited statutory law governed privacy and confidentiality in health care, which, unsurprisingly, produced inconsistent outcomes.[6] HIPAA, however, does not specify how to protect privacy or how to transmit health records efficiently and effectively. Instead, Congress delegated the responsibility for developing privacy standards to the Department of Health and Human Services (HHS) and mandated that HHS provide "detailed recommendations on standards with respect to the privacy of individually identifiable health information" within 12 months of HIPAA's enactment.[7] HIPAA further provided that if Congress failed to act on HHS's recommendations within 36 months of HIPAA's passage, the Secretary of HHS (Secretary) would administratively issue the final privacy regulations.[8]

With Congress unresponsive to its self-imposed deadline, HHS took up rulemaking and, after a period of public comment and modification, promulgated the HIPAA privacy[9] (privacy rules) and security[10] rules (collectively, the rules). The rules created, for the first time, minimum federal standards to address how health information may be used and safeguarded, and enumerated administrative patient privacy rights related to the information.[11] To safeguard individually identifiable health information (IIHI), the rules provide standards that explain the rights of individuals, procedures for the exercise of these rights, and the proper uses and disclosures of such information.[12] Significantly, the standards included an expanded range of disclosures that would be permissible without express patient authorization.[13] Thus, the HIPAA regulations that most observers have focused on, and the ones that most heavily impact staff counsel, are the privacy rules and their problematic and conditional preemption of state law.[14] Further discussion of the privacy rules will follow a brief overview of HIPAA.

Overview of HIPAA

Health care portability. Title I of HIPAA addresses health care access, portability, and renewability. This section creates a number

© 2008 by the American Bar Association. Reproduced by permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

of limits on health care plans,[15] including restrictions on preexisting condition exclusions.[16] A health insurance issuer or group health plan may only impose this exclusion if the individual received (or was recommended to receive) medical advice, diagnosis, care, or treatment for the condition in question within six months of the enrollment date.[17] Also, this exclusion cannot extend for more than 12 months after this date, and must be reduced if the individual had creditable coverage under another health plan.[18]

HIPAA also prohibits discrimination against individuals based on health status.[19] It states that an insurance provider may not establish eligibility rules for its plan based on an individual's health status, medical condition(s), claims experience, disability, or genetic information, among other things.[20] Other important features under this section are guaranteed coverage for small and large employers and the renewability of health coverage for employers and individuals.[21] All of these provisions help to increase health insurance availability and portability, and thus eliminate gaps in coverage.

Health care fraud and administrative simplification. The second title of HIPAA deals with reducing health care fraud and simplifying health care administration.[22] The section on health care fraud provides extensive guidelines for the exclusion of entities from participation in Medicare and state health programs. In most cases, the regulations also exclude entities previously convicted of health care fraud or found guilty of misconduct (e.g., losing one's license).[23] Administrative simplification appears under Subtitle F of Title II, from which the most far-reaching changes have grown. According to HIPAA, the purpose of this subtitle, in addition to improving Medicare and Medicaid, is to improve "the efficiency and effectiveness of the health care system by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[24] In other words, the Act was promulgated to reduce administrative costs and create standards for the protection of certain kinds of personal health information.

The reference to "certain kinds of health information" refers to individually identifiable health information or IIHI.[25] To qualify as IIHI, information must (1) be created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relate to (a) the past, present, or future health or condition of an individual, (b) the provision of health care to the individual, or (c) the past, present, or future payment for health care provided to the individual.[26] This information must also identify the individual or provide enough information to reasonably believe that it could be used to identify the individual.[27] According to HIPAA, three types of entities must follow the standards: health plans, health care clearinghouses, and health care providers.[28] These entities are defined as follows: A health plan is any individual or group plan that either pays for or provides medical care; a health care clearinghouse is an entity that processes health information from nonstandard to standard data elements; and a health care provider is any provider of medical or health services, such as a hospital.[29] These entities are referred to as "covered entities."[30]

Standards for electronic exchange of health information. The administrative simplification provision of HIPAA calls for the Secretary to create standards that improve the electronic transmission of health information and eliminate administrative waste. HIPAA requires the Secretary to produce regulations that create a uniform standard for electronic transactions; assemble unique health identifiers for each individual, employer, health care plan, and health care provider; and establish code sets for certain data elements (e.g., codes for each disease).[31] Additionally, the Secretary is to establish standards for maintaining proper security and privacy of individually identifiable health information.[32] At present, the above regulations are all in effect. However, the unique health identifier standards, known as the National Provider Identifier (NPI) Standard, only required compliance as of May 23, 2007. Small plans were given additional time and must be in compliance by May 23, 2008.[33]

Title II of HIPAA also outlines administrative, civil, and criminal penalties for violations of its standards, which are enforced by the Office for Civil Rights (OCR) of HHS.[34] The OCR handles administrative penalties, while the Department of Justice investigates criminal matters.[35] Although

---

Michael W. Drumke *is a partner with Schiff Hardin LLP in Chicago, specializing in products liability, mass/toxic tort claims, class actions, and environmental claims. He is a past chair of the TIPS Toxic Torts and Environmental Law Committee.* *He would like to acknowledge the assistance of Brian O. Watson and Michael Peluso for their help in preparing this article.* *Drumke can be reached at mdrumke@schiffhardin.com.*

© 2008 by the American Bar Association. Reproduced by permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

HIPAA does not provide for a private cause of action,[36] its regulations have been used to provide evidence of standards of care in state tort actions.[37]

Regarding administrative penalties, the Secretary may impose a civil fine of up to $100 for each violation, although the total fine amount for violations of the same regulation cannot exceed $25,000 per year.[38] These penalties, however, may not be imposed if the covered entity is not aware of the violation and could not have known about the violation by exercising reasonable diligence.[39] If a violation is due to reasonable cause and not willful neglect, the covered entity can fix the problem within 30 days to avoid any penalty.[40]

Criminal penalties may be imposed for violations of HIPAA when a person does any of the following three things: (1) use or cause to be used a unique health identifier, (2) obtain IIHI relating to an individual, or (3) disclose IIHI to another person.[41] The penalty for a violation pursuant to the act can be up to $50,000 and/or up to one year in prison. If the violation is committed under false pretenses, the person can be fined up to $100,000, receive a prison sentence of up to five years, or both. Finally, if the violation is committed with the intent to sell, transfer, or use IIHI for commercial gain, malicious harm, or personal gain, the person can be fined up to $250,000, sentenced up to ten years in prison, or both.[42]

Although the defined actions that constitute a violation of HIPAA seem straightforward, some confusion has arisen over whether the penalties can be applied to individuals or whether they only apply to covered entities. The Act uses "person" to describe who is subject to criminal penalties, and the Department of Justice has only prosecuted individuals for criminal offenses under HIPAA.[43] Attempting to elucidate the scope of criminal enforcement, the Office of Legal Counsel of the Department of Justice (OLC) issued a Memorandum Opinion[44] that discussed who can receive criminal penalties, but little clarity has been provided by the memorandum's interpretation, the Department of Justice's pursuits, and HIPAA's statutory language.[45]

The privacy rules. The privacy rules are codified at 45 C.F.R. §§ 160 and 164. Section 160 focuses on compliance and state law preemption and provides guidelines to covered entities, explaining the entity's responsibilities and the government's investigative procedures. The OCR can either conduct compliance reviews on its own initiative or respond to complaints.[46] Individuals who believe that a HIPAA violation has occurred can file a complaint within 180 days from the date they first knew of the violation, which the Secretary then investigates to determine if a violation has occurred.[47] The privacy rules state that the Secretary must pursue informal means of resolution whenever possible.[48] Thus far, the enforcement system has focused on responding to complaints rather than conducting compliance reviews to seek violations.[49]

Section 160 also addresses the important issue of conditional state law preemption. Unless state law relates to the privacy of IIHI and is more stringent than HIPAA and the privacy rules, state laws are expressly preempted.[50] The regulations state that "a state law is more stringent than HIPAA if it provides greater privacy protection for the individual who is the subject of the individually identifiable health information."[51] Expounding on this generality, the regulations explain that a state law is more stringent where (1) the state law prohibits or restricts a use or a disclosure of information while HIPAA would allow it; (2) the state law provides an individual with "greater rights of access or amendment" to medical information than provided under HIPAA; (3) the state law provides an individual with a "greater amount of information" about "a use, a disclosure, rights, and remedies" than provided under HIPAA; (4) the state law provides for retaining information for a longer duration or reporting more detailed information than provided under HIPAA; or (5) the state law otherwise "provides greater privacy protection for the individual who is the subject of the individually identifiable health information."[52] Thus, covered entities must remain attentive to both HIPAA and state regulations to determine whether to disclose protected health information (PHI). PHI is individually identifiable health information transmitted or maintained in electronic form that is specifically targeted by HIPAA and its security and privacy rules.[53]

Section 164 addresses both the security and privacy rules regarding PHI. The security rules generally obligate covered entities with certain responsibilities of risk management, such as restriction requirements for PHI access, physical and electronic safeguards, and contractual requisites for "business associates."[54] Section 160.103 defines a business associate as a person or company that works on behalf of a

© 2008 by the American Bar Association. Reproduced by permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

covered entity to perform activities that involve the use or disclosure of PHI.[55] The rule specifically names service-defined companies such as actuarial, data aggregation, and legal services.[56]

The second part of section 164 addresses the privacy rules,[57] which permit a covered entity to disclose PHI only to the individual to whom the information pertains for treatment, payment, or health care operations, or in response to a valid authorization.[58] Beyond these main exceptions, the privacy rules list a number of other situations where disclosure may be allowable, such as health care treatment of minors.

HIPAA also requires covered entities to follow a "minimum necessary" standard.[59] That is, whenever a covered entity uses or discloses PHI, it limits the disclosed information to the minimum necessary for accomplishing the stated purpose. This standard need not be applied in certain circumstances, including when the information is used for treatment, when the individual requests it, and when the disclosure is required by law.[60] For any other disclosure of PHI that does not fall under these exceptions, the covered entity must receive a written authorization from the individual in question.[61]

In addition, the privacy rules require covered entities to provide notice to their health care recipients of the entities' privacy practices so recipients are aware of their rights regarding PHI and how medical information may be used, disclosed, or amended.[62] About half of the people who sign the form do not read it, however, and of those who say they understand it, about one-third are unable to correctly answer questions about its terms.[63] The privacy rules also give individuals several important rights to help protect their PHI.[64] Individuals, for example, have the right to request that a covered entity restrict disclosures of their PHI, receive a copy of their PHI for inspection upon request, amend false information, and receive an accounting of all disclosures of their PHI.[65]

Business associate contracts. HIPAA allows covered entities to share information with business associates provided they receive "satisfactory assurances" that the business associates will safeguard the privacy of any PHI they receive.[66] These satisfactory assurances must be documented through written contract, referred to as a "business associate contract."[67] The business associate contract generally assigns the business associate with the same privacy rules duties as the covered entity, except the business associate would not be liable for HIPAA violations. However, violations involving PHI can lead to the cancellation of the business associate contract and, depending on the wording of the contract, liability for any losses the covered entity incurs as a result of the associate's conduct.[68]

A covered entity will not be in compliance with HIPAA if it knows of a violation by a business associate and fails to notify the business associate; it will also not be in compliance if it fails to take reasonable steps to cure the violation, terminate the contract, or report the violation to HHS when termination is not feasible.[69]

If a law firm or law department is working with a covered entity and requires the use of PHI, the firm or department will probably require a business associate contract with the covered entity. For example, although HIPAA includes "legal services" under its definition of health care operations, the vagueness of the term means that most health care providers may require business associate contracts to ensure that they comply with HIPAA.[70]

Thus, attorneys who use or disclose PHI must ensure compliance with HIPAA, such as restricting disclosures and, when disclosure is necessary, using the "minimum necessary" standard. One possible stumbling block for law firms or law departments acting as business associates under HIPAA is that any PHI should be returned to the covered entity or destroyed, if feasible, once the contract is ended.[71] Due to most law firms' policies of file maintenance, compliance requirements could prove problematic, but such considerations may declare these terms "unfeasible" under attorney-client privilege.[72]

Constitutional Challenges to HIPAA

In *South Carolina Medical Association v. Thompson*,[73] the plaintiffs pursued a tripartite challenge to the constitutionality of HIPAA. First, the plaintiffs asserted that enactment of HIPAA violated the nondelegation doctrine because Congress failed to provide an intelligible principle to guide HHS.[74] Second, the privacy rules, as plaintiffs alleged, exceeded the scope of authority granted by Congress to HHS because they attempt to regulate medical records other than those transmitted electronically.[75] Finally, the plaintiffs postulated that the nonpreemption of "more stringent" state privacy laws was unconstitutionally vague, in violation of the Due Process Clause of the Fifth Amendment.[76] The U.S. District Court for the District of South Carolina dismissed the suit, and the plaintiffs appealed.

© 2008 by the American Bar Association. Reproduced by permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

The Fourth Circuit rejected all three arguments and affirmed the district court's decision. With respect to the nondelegation doctrine, the Fourth Circuit found that HIPAA contained the requisite intelligible principle to guide HHS (notably, by requiring HHS to focus on three particular subjects).[77] Addressing the second claim, the court noted that restricting HIPAA to the regulation of only electronic information was not stated in the act and, had HIPAA stated this restriction, it would prevent HIPAA from accomplishing its privacy protection aim.[78] Finally, the court concluded that the standards set forth by HHS for determining whether or not a state law is preempted are "sufficiently definite to give fair warning as to what will be considered" preempted and that no more is required.[79]

The Impact of HIPAA on Litigation and State Regulations

Subpoenas and protective orders. Because of HIPAA's privacy rules, attorneys cannot simply issue traditional subpoenas or discovery requests to obtain PHI; HIPAA maintains explicit allowances for disclosures of PHI pursuant to judicial and administrative proceedings.[80] Covered health care entities, however, may request a statement to ensure that the attorney has made a good faith effort to either notify the individual who is the subject of the PHI or secure a qualified protective order.[81] The protective order must prohibit the use of the PHI for any purpose other than the litigation in question, and must provide for the return or destruction of the PHI at the end of the litigation. Acknowledging the complexity of HIPAA and the tendency for covered entities to err on the side of caution, attorneys wishing to acquire PHI should obtain either a court order or a qualified protective order.[82]

National Abortion Federation, et al. v. Ashcroft[83] addressed whether Illinois law provided for more restrictive medical information disclosure and therefore superseded the application of HIPAA. This case stemmed from another matter in New York, where the National Abortion Federation brought a civil action against the U.S. attorney general. The action challenged the constitutionality of the Partial Birth Abortion Ban based on the fact that it did not have an exception for cases in which a woman's health was in danger. Dr. Cassing Hammond, a plaintiff in the suit, asserted that he had performed abortions banned under the contested act to protect his patients' health. Shortly thereafter, the U.S. attorney general served Hammond with requests for the medical records of the women who had received those abortions. When told that Northwestern Memorial Hospital in Chicago, Illinois, had the records, the government served the hospital with a subpoena for the records accompanied with a court order. The New York judge, who presided over the New York case, issued a protective order allowing the hospital to redact certain identifying information to safeguard privacy. Northwestern Memorial Hospital then moved to quash the subpoena under both HIPAA and Illinois law, and the U.S. District Court for the Northern District of Illinois granted its request.[84]

The court's decision to quash the subpoena referred to the Illinois Code of Civil Procedure, which contains the "physician-patient privilege."[85] This privilege provides that a physician may not disclose any information gathered while attending a patient unless one of eleven conditions exists. If these conditions do not exist, the records cannot be disclosed without the patient's written consent.[86] The court found that Illinois privacy law is more stringent than HIPAA, because it generally requires written consent from the patient in order to release information, with provisions for civil suits against entities that disclose PHI in violation of Illinois law.[87] The government appealed the decision to quash the subpoena.

The Seventh Circuit upheld the order quashing the subpoena, but on the grounds that the subpoena imposed an undue burden on Northwestern Memorial Hospital under Federal Rule of Evidence 501. The Seventh Circuit disagreed with the lower court's reasoning, claiming that the HIPAA regulations do not allow state evidentiary privileges to govern federal question lawsuits.[88] It seems, therefore, that Illinois law is not preempted by HIPAA, but the issue is not completely clear.

The New York courts, however, sharply diverged from the decision of the Seventh Circuit.[89] The district court stated that "Congress has spoken on the privacy of medical records through HIPAA."[90] The court reasoned that the protective order issued by the lower court constituted a "qualified protective order," as defined by HIPAA.[91] Therefore, the hospital records were disclosed because the HIPAA regulations permitted the release of information after a protective order was obtained.

Ex parte communications

© 2008 by the American Bar Association. Reproduced by permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

under HIPAA. While federal jurisprudence grows on the issue of ex parte communications under HIPAA, the existing case law supports a finding that such contact should be allowed when a court order grants the communication.[92] For example, in *Bayne v. Provost*, the federal district court surveyed the sparse jurisprudential landscape to determine that HIPAA created no bright line rule barring all ex parte discussions.[93] In *Bayne*, a civil rights and false imprisonment action, the court evaluated whether the defendants may conduct an interview of a nurse practitioner who had visited and engaged in telephone conversations as part of a home treatment program with the plaintiff prior to his hospital transport and detention.[94] The *Bayne* court found that state privileges do not apply in federal question cases, but then proceeded to analyze whether New York law was more stringent than the protections provided by HIPAA.[95] Granting a qualified protective order and authorization to interview the nurse practitioner, the court found that New York law did not offer more protections and was thus preempted by HIPAA, while implying that if it had found the reverse the court would have applied New York confidentiality law to the federal question case.[96]

Since *Bayne*, the jurisprudential landscape remains uncertain with no bright line rule. In an unpublished opinion, the federal court in Kansas determined that a court order clearly allows the production of medical information and ex parte contact when all the requirements of HIPAA are met.[97] In *Vioxx MDL*, the court found the just option was to protect the relationship between a doctor and patient by restricting the defendants from conducting ex parte communications with plaintiffs' treating physicians while allowing plaintiffs' counsel to engage in ex parte interviews with those doctors who had not been named as defendants.[98] Most recently, the Supreme Court of Oklahoma found HIPAA does not expressly bar ex parte communications, but requires any court order to contain clearly permissive and specific language that does not contravene HIPAA's confidentiality requirements.[99]

The "minimum necessary" standard. Recent HIPAA litigation provides some guidance and clarification with respect to the Act's "minimum necessary" standard.[100] In *Acosta v. Byrum*, the plaintiff cited HIPAA as the determinant for the appropriate level of care in relation to the privacy of medical information.[101] Acosta sued both Dr. Faber, his psychiatrist, and Robin Byrum, an office assistant, alleging that Faber allowed Byrum to use his access code to view Acosta's psychiatric records and that Byrum disclosed this information to third parties. The negligence action arose, in part, from Byrum's use of the access code in a way that violated the HIPAA standard of privacy. The trial court dismissed Acosta's action.[102]

The appeals court reversed the trial court's dismissal, finding that the action was not a medical malpractice claim but was based on the administrative conduct of the psychiatrist in permitting a staff member to view a patient's record by use of the physician's access code. The court acknowledged that HIPAA provided no private right of action; however, HIPAA may be used to establish an appropriate standard for the protection of health care information.[103] Thus begins what may likely be a line of civil cases using HIPAA as a standard for measuring the duty to maintain health care privacy.

Enforcement of HIPAA. Although the criminal enforcement provisions related to HIPAA set the stage for criminal prosecutions against violators, the Department of Justice had prosecuted only four criminal HIPAA violations as of February 13, 2007.[104] During that four-year period over 350 complaints were considered by the Department of Justice, with the Office of Civil Rights referring a total of 366 complaints to the Department of Justice for investigation of potential criminal violations. None of the prosecuted cases, however, originated from OCR referrals, and none of the 24,500 complaints received by OCR through its privacy complaint system resulted in the imposition of civil penalties.[105]

In November 2004, the first prosecution for violations of HIPAA concluded with the conviction of Richard Gibson, who stole a patient's personal information and then used it to obtain credit cards in the patient's name.[106] With these cards, Gibson illegally charged some $9,000. Gibson then entered into a plea agreement with the government, which required him to pay for the patient's credit card debt and expenses and to serve 10 to 16 months in prison.[107] The second conviction was Liz Ramirez in Texas, who worked in the office of a physician who provided physical examinations and medical treatment to FBI agents.[108] An undercover investigator posed as a drug trafficker to buy PHI on a particular FBI agent for a $500 payment to Ramirez. Officers then

© 2008 by the American Bar Association. Reproduced by permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

arrested and charged her with violating HIPAA.[109]

More recently, a widely publicized south Florida case involved Isis Machado, a former employee of Cleveland Clinic Hospital, who printed out the PHI of over 1,100 patients and passed them to her cousin, Fernando Ferrer, who happened to own a claims company.[110] Through that company, Ferrer filed over $2.5 million in fraudulent Medicare claims. With testimony against Ferrer negotiated, Machado pled guilty to conspiracy and received a reduced sentence of three years' probation, including six months of home confinement. Ferrer pled not guilty but was found guilty and sentenced to seven years and three months in prison. The defendants were ordered to make restitution of a combined $2.51 million to the government.[111]

Recommendations for Sound HIPAA Policy

HIPAA and its provisions significantly affect covered entities, business associates, law firms and departments, hospital employees, and patients. To date, the government has permitted violations to go unpenalized.[112] However, with privacy advocates criticizing the relative lack of enforcement and health care receiving increased political attention, prosecutions and fines will likely increase. Impacted institutions must ensure sufficient security measures, proper training methods, and appropriate authorization forms and contracts. As interpretations of HIPAA's provisions evolve, they must also remain current on new developments, from both state and federal regulators, and adjust their procedures accordingly. Institutions with clear policies and effective training programs will minimize the risk of HIPAA violations.

For law firms or law departments, individual attorneys and their staff need to follow proper procedures for obtaining and controlling PHI. When obtaining a court order or a qualified protective order, attorneys should draft clearly permissive language to ensure effective, jural discovery. A law firm or law department that handles PHI for a covered entity will probably require a business associate contract, but subrogation provisions in the contract should be avoided. When handling PHI, attorneys and their staff must use and disclose only the necessary information, and should investigate possible unauthorized disclosures. In sum, those who deal with PHI should be aware of HIPAA, its regulations, and the forms and actions required to ensure compliance. ■

Notes

1. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in various sections of Titles 18, 26, 29, and 42 of the United States Code) [hereinafter referred to as HIPAA].

2. The Clinton Administration Description of President's Health Care Reform Plan, *American Health Security Act of 1993*, dated Sept. 7, 1993, obtained by the Bureau of National Affairs on Sept. 10, 1993.

3. 45 C.F.R. § 160.101 (2003) (implementing sections 1171 through 1179 of the Social Security Act (42 U.S.C.A. §§ 1320d through 1320d-8)).

4. HIPAA, *supra* note 1, at pmbl.

5. *See* Tamela J. White & Charlotte A. Hoffman, *The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos*, 106 W. VA. L. REV. 709, 713 (2004).

6. *See generally id.*

7. HIPAA, *supra* note 1, at § 264.

8. *Id.*

9. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,182 (Aug. 14, 2002).

10. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8333, 8334 (Feb. 20, 2003) (to be codified at 45 C.F.R. §§ 160, 162, 164; finalized in 45 C.F.R. §§ 160, 162, 164 (2003)).

11. 45 C.F.R. § 164.520(b) (2003); *see also* Scott D. Stein, *What Litigators Need to Know About HIPAA*, 36 J. HEALTH L. 433, 433 (2003) (describing the purpose of the HIPAA privacy standards).

12. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. §§ 160, 164 (2003)).

13. 45 C.F.R. §§ 164.506, 164.512, 164.520 (2003).

14. *See, e.g.*, Rebecca Bishop, *The Final Patient Privacy Regulations Under the Health Insurance Portability and Accountability Act—Promoting Patient Privacy or Public Confusion?*, 37 GA. L. REV. 723, 724–25 (2003).

15. Linda E. Rosenzweig, *The New Regulations Under the Health Insurance Portability and Accountability Act of 1996*, 14 THE HEALTH LAW. 28–34 (Jan. 2002).

16. 26 U.S.C. § 9801 (West 2008); *see also* Rosenzweig, *supra* note 15, at 30–31.

17. *See* 42 U.S.C. § 300gg; 29 U.S.C. § 1181; 26 U.S.C. § 9801.

18. 42 U.S.C. § 300gg.

19. *See* 42 U.S.C. § 300gg-1; 29 U.S.C. § 1182; 26 U.S.C. § 9802.

20. *See* 42 U.S.C. § 300gg-1; 29 U.S.C. § 1182; 26 U.S.C. § 9802.

21. *See* 42 U.S.C. §§ 300gg-11, 300gg-12, 300gg-42.

22. HIPAA, Title II, Subtitle F comprises sections 261 through 264. Section 261, codified at 42 U.S.C. §

© 2008 by the American Bar Association. Reproduced by permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

1320d note, states the purpose of the subtitle. Section 262 amends Title XI of the Social Security Act, 42 U.S.C. §§ 1301 *et seq.*, to add Part C, "Administrative Simplification," with sections 1171 through 1179, codified at 42 U.S.C. §§ 1320d through 1320d-8. Section 263 amends the Public Health Service Act at 42 U.S.C. § 242k(k). Section 264 is codified at 42 U.S.C. § 1320a-7.

23. 42 U.S.C. § 1320a-7.

24. HIPAA, *supra* note 1, at § 261; *but see* S.C. Med. Ass'n v. Thompson, 327 F.3d 346, 353 (4th Cir. 2003), *cert. denied*, 540 U.S. 981 (2003) ("[t]he plain language of HIPAA indicates that HHS could reasonably determine that the regulation of individually identifiable health information should include [electronic and] non-electronic forms of that information").

25. *See* 45 C.F.R. § 160.103 (defining an individual's "protected health information" as individually identifiable health information maintained in or transmitted in any form or media including electronic media—except as otherwise provided by the rule).

26. 42 U.S.C. § 1320d(6).

27. *Id.* at § 1320d(6).

28. *Id.* at § 1320d-1(a).

29. *Id.* at § 1320d(2),(3), (5).

30. 45 C.F.R. § 160.103.

31. *Id.* at § 1320d-2.

32. *Id.*

33. HIPAA Administrative Simplification: Standard Unique Health Identifier for Health Care Providers, 69 Fed. Reg. 3434–3469 (Jan. 23, 2004) (finalized at 45 C.F.R. § 162).

34. *See* HIPAA, *supra* note 1, § 1176(a) (outlining civil penalties for violating sections of part C); *id.* § 1177 (outlining criminal penalties for anyone who knowingly misuses a unique health identifier, or obtains or discloses individually identifiable health information).

35. Doreen Z. McQuarrie, *HIPAA Criminal Prosecutions: Few and Far Between*, HEALTH L. PERSP., Feb. 19, 2007, *available at* www.law.uh.edu/healthlaw/perspectives/2007/(DM)HIPAACrimCharges.pdf (last visited Feb. 21, 2008) (noting that 366 matters were sent to the Department of Justice for enforcement and four individuals were prosecuted for criminal offenses).

36. *See, e.g.*, Bagent v. Blessing Care Corp., 844 N.E.2d 469, 472 (Ill. App. Ct. 2006) (citing Univ. of Colo. Hosp. Auth. v. Denver Publ'g Co., 340 F. Supp. 2d 1142, 1145 (D. Colo. 2004)).

37. *See, e.g.*, Acosta v. Byrum, 638 S.E.2d 246, 253 (N.C. Ct. App. 2006) (plaintiff citing HIPAA as evidence of the appropriate standard of care in negligence action).

38. 42 U.S.C. § 1320d-5.

39. *Id.*

40. *Id.*

41. 42 U.S.C. § 1320d; *see also* McQuarrie, *supra* note 35, at 1.

42. 42 U.S.C. § 1320d.

43. *See* McQuarrie, *supra* note 35, at 1.

44. *See* Memorandum Opinion for The General Counsel Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General on the Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6 (June 1, 2005), *available at* www.usdoj.gov/olc/hipaa_final.htm.

45. *See* AIS Compliance, *HIPAA Compliance Strategies—HIPAA Criminal Cases Against Individuals Proceed Despite DOJ Memo*, *available at* www.aishealth.com/Compliance/Hipaa/RPP_HIPAA_Cases_Proceed.html; Peter P. Swire, *Justice Department Opinion Undermines Protection of Medical Privacy*, Center for American Progress (June 7, 2005), *available at* www.americanprogress.org/issues/2005/06/b743281.html.

46. 45 C.F.R. §§ 160.306, 160.308.

47. *Id.* at § 160.306.

48. *Id.* at § 160.312.

49. Rob Stein, *Medical Privacy Law Nets No Fines: Lax Enforcement Puts Patients' Files at Risk, Critics Say*, WASH. POST, June 5, 2006, at 2.

50. 45 C.F.R. § 160.203; *see, e.g., S.C. Med. Ass'n*, 327 F.3d at 355; *In re* Diet Drug Litig., 895 A.2d 493, 499–501 (N.J. Super. Law Div. 2005); Crenshaw v. MONY Life Ins. Co., 318 F. Supp. 2d 1015, 1028 (S.D. Cal. 2004); Law v. Zuckerman, 307 F. Supp. 2d 705, 708 (D. Md. 2004); Nat'l Abortion Fed'n v. Ashcroft, 2004 WL 292079 at *2–3 (N.D. Ill. Feb. 6, 2004); United States *ex rel.* Stewart v. La. Clinic, 2002 WL 31819130 at *3 (E.D. La. 2002); Allen v. Wright, 644 S.E.2d 814, 816–17 (Ga. 2007); Findley v. Findley, 937 So. 2d 912, 916 (La. Ct. App. 2006), *writ denied*, 938 So. 2d 88 (La. Sup. Ct. 2006); Northlake Med. Ctr., LLP v. Queen, 634 S.E.2d 486, 489 (Ga. 2006).

51. *See, e.g., S.C. Med. Ass'n*, 327 F.3d at 355 (quoting 45 C.F.R. § 160.202).

52. *Id.*

53. 45 C.F.R. § 160.203.

54. *Id.* at § 164.302.

55. *Id.* at § 160.103.

56. *Id.*

57. *Id.* at § 164.502.

58. *Id.*

59. *Id.* at § 164.502(b).

60. *Id.*

61. *Id.* at § 164.508.

62. *Id.* at § 164.520; *see also* Office for Civil Rights, U.S. Dep't of Health & Human Servs., *OCR Guidance Explaining Significant Aspects of the Privacy Rule*, 40–41 (rev. ed. 2003), *available at* www.hhs.gov/ocr/hipaa/guidelines/notice.pdf (last visited Feb. 21, 2008).

63. *See* Epictide, Inc., *Medical Identity Theft Consumer Study Survey Results* (2006), *available at* www.epictide.com/documents/2006-1212-Consumer-Survey.pdf (last visited Feb. 21, 2008).

64. *See* 45 C.F.R. §§ 164.522–28.

© 2008 by the American Bar Association. Reproduced by permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

65. *Id.*

66. *Id.* at § 164.504(e)(2).

67. *Id.*

68. *See* Kim C. Stanger, *HIPAA Privacy and Security for Employers: An Alert and Quick Overview*, 48-MAY ADVOCATE (Idaho), 27, 28 (2005) (explaining the penalties resulting from violations).

69. 45 C.F.R. § 164.504(e)(1).

70. *Id.* at § 164.501.

71. *Id.* at § 164.504(2)(i)(I).

72. *See* Alexander L. Bednar, *Potential Abrogation of Attorney-Client Privilege in Oklahoma as a Result of HIPAA*, 57 OKLA. L. REV. 813, 816–17 (2004) (noting possible problems with provisions of business associate contracts).

73. 327 F.3d 346 (4th Cir. 2003).

74. *Id.* at 349.

75. *Id.*

76. *Id.*

77. *Id.* at 351.

78. *Id.* at 353-54.

79. *Id.* at 355.

80. 45 C.F.R. § 164.512(e)(1)(i).

81. *Id.* at § 164.512(e).

82. *Id.*

83. 2004 WL 292079 at *1, *aff'd on other grounds*, Nw. Memorial Hosp. v. Ashcroft, 362 F.3d 923, 925 (7th Cir. 2004) (affirming because the district court's quashing of subpoena by Fed. R. Evid. 501 and the HIPAA regulations do not impose state evidentiary privileges on suits to enforce federal law, as well as decisions arising from state law).

84. *Id.*

85. *Id.* at *2.

86. *Id.* (citing 735 ILCS 5/8-802).

87. David Humiston & Stephen M. Crane, *Will Your State's Privacy Law Be Superseded by HIPAA?*, 11:5 MANAGED CARE 1, 6 (May 2002).

88. *Nw. Memorial Hosp.*, 362 F.3d at 925.

89. Nat'l Abortion Fed'n v. Ashcroft, 2004 WL 555701, at *6–7 (S.D.N.Y. March 19, 2004), *aff'd sub nom.* Nat'l Abortion Fed'n v. Gonzales, 224 Fed. Appx. 88, 2007 WL 1454322, (2d Cir. (N.Y.) May 16, 2007).

90. *Id.* at *6.

91. *Id.* at *7.

92. *See* Bayne v. Provost, 359 F. Supp. 2d 234, 240 (N.D.N.Y. 2005) (permitting ex parte communications with health care providers when "court order" exception to HIPAA was present); *In re* Vioxx Products Liab. Litig., 230 F.R.D. 473, 477 (E.D. La. 2005), *aff'd on other grounds*, 2005 WL 2036797 (E.D. La. 2005) (restricting defendants from conducting ex parte communications but allowing plaintiffs' counsel to engage in ex parte interviews with those doctors who have not been named as defendants.); *but see*, *Crenshaw*, 318 F. Supp. 2d at 1028 (providing that HIPAA does not authorize ex parte contacts with health care providers); *Zuckerman*, 307 F. Supp. 2d at 712 (precluding defense counsel from having any further ex parte communications with physician was not warranted).

93. *Bayne*, 359 F. Supp. 2d at 239.

94. *Id.* at 235.

95. *Id.* at 238–41.

96. *See id.* at 239–41.

97. Hulse v. Suburban Mobile Home Supply Co., 2006 WL 2927519 (D. Kan. 2006).

98. *In re Vioxx*, 230 F.R.D. at 477.

99. Holmes v. Nightingale, 2007 OK 15, 158 P.3d 1039 (2007).

100. 45 C.F.R. § 164.502(b).

101. 638 S.E.2d 246 (N.C. Ct. App. 2006).

102. *Id.* at 249.

103. *Id.* at 253.

104. *See* McQuarrie, *supra* note 35, at 1.

105. *Id.*

106. United States v. Gibson, No. CR04-0374RSM, 2004 WL 2237585 (W.D. Wash. Aug. 19, 2004).

107. *Id.*

108. United States v. Ramirez, No. 7:05CR00708 (S.D. Tex. Aug. 30, 2005); *see also* Press Release, Dep't of Justice, *Alamo Woman Convicted of Selling FBI Agent's Medical Records* (Mar. 7, 2006), *available at* www.usdoj.gov/usao/txs/releases/March2006/060307-Ramirez.pdf.

109. *Id.*

110. United States v. Ferrer, No. 06-60261 CR-COHN (S.D. Fla. Sept. 7, 2006); *see also* Press Release, Fed. Bureau of Investigation Miami Field Div., *Naples Man Convicted in Cleveland Clinic Identity Medicare Fraud Case* (Jan. 24, 2007), *available at* http://miami.fbi.gov/dojpressrel/pressrel07/mm20070124b.htm.

111. *Id.*

112. In an audit of a hospital performed by the HHS, the Office of the Inspector General of HHS presented Piedmont Hospital in Atlanta a list of 42 items that the HHS wanted information within ten days. *See* Jaikumar Vijayan, *HIPAA Audit: The 42 Questions HHS Might Ask*, COMPUTERWORLD, *available at* www.computerworld.com, for a list of the questions (last visited Feb. 21, 2008).

© 2008 by the American Bar Association. Reproduced by permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.