Annals of Health Law

Volume 12
Issue 1 *Winter 2003*

Article 7

2003

Time Is Running Out - The Burdens and Challenges of HIPAA Compliance: *A Look at Preemption Analysis, the Minimum Necessary Standard, and the Notice of Privacy Practices*

Jennifer Guthrie

Time Is Running Out—The Burdens and Challenges of HIPAA Compliance: *A Look at Preemption Analysis, the "Minimum Necessary" Standard, and the Notice of Privacy Practices*

Jennifer Guthrie

I. Introduction to HIPAA: Its Benefits, Its Burdens

Privacy is a matter that touches all of our lives. We shut the door when speaking on the telephone. We keep our personal life separate from our work life. We speak in low whispers on a crowded bus. The privacy concerns regarding our private health information, however, may stir even more intense feelings. Personal information regarding the ailments that afflict us, or the therapy that cures us, deserves a special kind of shield. Moreover, every one of us should have the right to determine when this information may be divulged to others.

Many Americans fear extreme embarrassment if their health information is used or disclosed. In fact, one out of every six adults in the United States says that they have done something out of the ordinary to keep personal medical information confidential.[1] Some patients may limit the information they disclose to their health care provider; others may outright lie. Patients may seek multiple providers so that their medical record is not consolidated; some may avoid treatment all together. Obviously, these privacy-protective behaviors can have an adverse effect upon patient care. In 1996, Congress recognized the need for national privacy standards, and in response enacted the Health Insurance Portability and Accountability Act ("HIPAA").[2] This law, which is applicable to health plans,

1. This statistic was pursuant to a poll conducted for the California HealthCare Foundation in Jan. 1999. Janlori Goldman & Zoe Hudson, *Exposed: A Health Privacy Primer for Consumers*, Health Privacy Project, Dec. 1999, with support from the Open Society Institute's Program on Medicine as a Profession, *available at* http://www.healthprivacy.org/usr_doc/33806.pdf.

2. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.); 42 U.S.C. § 1320d -1320d-8 (West Supp. 1998).

health care clearinghouses, and health care providers[3] was an important step in the protection of privacy.[4] The burdens and challenges of its implementation, however, pose serious obstacles to the goal of final compliance.

The HIPAA framework is actually quite simple in that the statute sets forth general guidelines for future action.[5] Specific to this discussion, HIPAA mandated the passage of comprehensive privacy legislation by Congress within three years, otherwise the Department of Health and Human Services ("HHS") was required to step in and create privacy regulations.[6] In the event that HHS intervened, Congress expressly required that three specific areas of privacy be addressed:

(1) An individual's right with respect to his or her health information,
(2) the procedures that must be established in order to exercise those rights, and
(3) the uses and disclosures of health information that should be authorized or required.[7]

When Congress failed to develop any sort of succeeding legislation, HHS responded with an expansive array of definitions, re-

3. HIPAA applies only to those health care providers "who transmit any health information in electronic form . . .."; 42 U.S.C. § 1320d-1(a)(3); 45 C.F.R. § 160.102(a)(3) (2002). Practically speaking, most providers electronically transmit information in some capacity, thus making them subject to HIPAA.

4. In addition to privacy, HIPAA also mandates the creation of standards with respect to (1) transactions, (2) security, (3) identification, and (4) enforcement. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.); 42 U.S.C. § 1320d to 1320d-8 (West Supp. 1998).

5. The preamble to HIPAA states that the Act was created "[t]o amend the Internal Revenue Code of 1986 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 services and coverage, to simplify the administration of health insurance, and for other purposes." Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936) (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.); 42 U.S.C. § 1320d-1320d-8 (West Supp. 1998). Interestingly, the focus on privacy has swamped the accomplishment of the titular goals set forth in the Act.

6. 42 U.S.C. § 1320d-2 note (Section 264(c)(1) of Public Law 104-191) provides, "[I]f legislation governing standards with respect to the privacy of individually identifiable health information . . . is not enacted by a date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act."

7. *See* 42 U.S.C. § 1320d-2 note (Section 264(b) of Public Law 104-191).

quirements, and exceptions necessary for implementation and compliance.[8] These are known as the "Privacy Regulations."[9]

Covered entities are required to comply with the Privacy Regulations by a compliance date of April 14, 2003.[10] Health plans, health care clearinghouses, and health care providers will be

8. Standards for Privacy of Individually Identifiable Health Information (hereinafter "Privacy Rule"), 45 C.F.R. Parts 160 and 164; 65 Fed. Reg. 82,462 (Dec. 28, 2000). HHS proposed federal privacy standards in 1999 and, after reviewing and considering more than 50,000 public comments on them, published final standards on Dec. 28, 2000. Press Release, *HHS Issues First Guidance on New Patient Privacy Protections*, U.S. Dep't of Health & Human Servs., July 6, 2001. Also note that compliance with the regulations is not required for most entities until 24 months from the effective date of the final rule. Normally, the effective date is 60 days after a rule is published. In this case, however, a paperwork glitch delayed the effective date until Apr. 14, 2001, and thus compliance for most covered entities is not required until Apr. 14, 2003; HIPAA Primer, Phoenix Health Systems, *available at* http://www.Hipaadvisory.com/regs/hipaaprimer1.htm.

9. The breadth of these regulations has stirred much debate in the health care industry. Many argue that HHS has exceeded its constitutional authority by issuing an extensive and overly burdensome set of regulations. In the past, some groups even filed suit against the Department for crafting regulations beyond the guidance provided by Congress. According to allegations by the South Carolina Medical Association (hereinafter "SCMA"), the Physicians Care Network, and several individual physicians, HHS assumed a broad lawmaking role that is constitutionally delegated to the legislative branch. By acting as "federal legislators," HHS overstepped its bounds and was given an impermissible delegation of legislative authority. The SCMA alleged, "We're fighting this to enforce the Constitution . . . if we win, medical privacy is going to get thrown back into the Congress. Then at least we can have some input with our . . . representatives. With the bureaucratic arm, we have no input at all." Amy Snow Landa, *HHS Sued Over Medical Privacy Rules*, American Medical News, Aug. 6, 2001. On Aug. 14, 2002, the federal district court for South Carolina dismissed the constitutional claims made by the SCMA and there have been no appeals as of present. Similar lawsuits were also filed, including a constitutional challenge by the Association of American Physicians and Surgeons (hereinafter "AAPS"), Congressman Ron Paul, M.D. (R-TX), and three individual patients. *See* Assoc. of Am. Physicians & Surgeons, Inc. v. U.S. Dep't of Health & Human Servs., No. 01-CV-2963, 2002 WL 1917633 (S.D. Tex., July 17, 2002). This group took a different angle than the SCMA and challenged the HIPAA Regulations based on their content. For example, the complaint claimed that HIPAA violates the Fourth Amendment by requiring physicians to turn over medical records without a warrant and by authorizing the government to construct a database that includes personal health identifiers. Tanya Albert, *Second Group Files Suit Over Privacy Rules*, American Medical News, Aug. 20, 2001; *see also* http://www.aapsonline.org, for a link to the *AAPS v. HHS* lawsuit information, including an online copy of the complaint at law. Similar to the SCMA suit, a Texas federal court recently dismissed this constitutional challenge as well. No appeals are on record.

10. 45 C.F.R. § 164.534(a) (2002). Small health plans are held to a compliance date of Apr. 14, 2004. 45 C.F.R. § 164.534(b)(2) (2002). Small health plans are defined as "health plan[s] with annual receipts of $5 million or less." 45 C.F.R. § 160.103 (2002). Note that the compliance date in the final rule is actually published Feb. 26, 2003 (Feb. 26, 2004 for small health plans). The compliance date is recognized as Apr. 14, 2003 (Apr. 14, 2004 for small health plans).

forced to undergo substantial operational changes in order to comply. New policies and procedures must be implemented, in accordance with the regulations. Systems need to be created, employees need to be trained, and consent forms need to be printed. In the end, covered entities will spend considerable time and money in order to ensure compliance by the April 2003 deadline.[11]

But what, exactly, are the benefits of these new regulations? The main premise of HIPAA is to protect individually identifiable health information. This means that certain information will not be revealed without a patient's express authorization, in an effort to contain important information to as few people as possible.[12] In its entirety, HIPAA has set forth a wave of improvements with regard to individual patient benefits. The Privacy Regulations incorporate a remarkable list of "Patient Rights," which includes the right of access to medical records, to amend medical records, and to complain of a covered entity's policies and procedures.[13] In sum, HIPAA impacts the patient in a variety of beneficial ways.

There are, however, burdens to these benefits. While patients enjoy newfound privacy protections, covered entities must adhere to significant and costly compliance requirements.[14] Three

11. The estimated cost of compliance with the final rule is $17.6 billion over the ten-year period from 2003-2012. This includes the costs for all the major requirements for the rule, including costs to federal, state, and local governments. These costs reflect the changes that affected organizations will have to undertake to implement and maintain compliance with the requirements of the rule and achieve enhanced privacy of protected health information. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,760 (Dec. 28, 2000).

12. *See* 45 C.F.R. § 164.508 (2002). "Uses and disclosures for which an authorization is required." The final modification of the Privacy Regulations removed mandatory consent and made it discretionary for covered entities. 45 C.F.R. § 164.506 (2002).

13. There are six main categories of 'Patient Rights': (1) the right to a notice of privacy practices for protected health information, (2) the right to request privacy protection of protected health information, (3) the right of access to protected health information (inspect and copy), (4) the right to amend protected health information, (5) the right to an accounting of disclosures of protected health information, and (6) the right to complain to a covered entity regarding policies and procedures of that entity. 45 C.F.R. §§ 164.520, 164.522, 164.524, 164.526, 164.528, 164.530(d)(1) (2002).

14. Compliance is critical in order to avoid HIPAA penalties. The statute imposes civil penalties of $100 per violation, up to $25,000 per year for each requirement or prohibition violated. Congress also established criminal penalties for certain actions, such as obtaining or disclosing individually identifiable health information, in violation of the law. Criminal penalties are up to $50,000 or one year in prison for certain offenses, or both; up to $100,000 or up to five years in prison, or both if the offenses committed are under "false pretenses"; and up to $250,000 or up to ten years in prison

challenging and burdensome obstacles will be highlighted in this paper: (1) preemption analysis, (2) the "minimum necessary" standard, and (3) the Notice of Privacy Practices. Each obstacle is a significant component of the Privacy Regulations and among the most debated topics among HIPAA critics.[15] Therefore, the discussion below focuses on these critical issues and explores possible alternatives and suggestions to make compliance less burdensome.

First, preemption analysis will be discussed. In terms of the expectations of covered entities, preemption is perhaps the greatest burden placed upon them. In any given situation, covered entities must perform an analysis that determines whether federal law preempts state privacy law. This paper argues that the covered entities are not trained in legal analysis, and should not be required to utilize considerable time or resources in order to ensure compliance. Instead, focusing on patient care should continue to remain their top priority.

Another major challenge for covered entities concerns the "minimum necessary" standard required by the Privacy Regulations. Covered entities must make "reasonable efforts" to limit the use, disclosure, or request of protected health information to what is minimally necessary.[16] While there are many exceptions to this general rule, provider "uses" of information for treatment purposes remains subject to the standard. This increases both the burden of compliance and the risk of significant detriment to patient care. Further, since the term "reasonable" may be assessed by the covered entities themselves,[17] the standard

---

if the offenses are committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in sections of 18, 26, 29 and 42 U.S.C.); 42 U.S.C. § 1320d - 1320d-8 (West Supp. 1998).

15. Other hotly debated issues include limitations on potential research, inclusion of oral communications, business associate issues, and non-protective marketing requirements. *See, e.g.*, Bernadette M. Broccolo & Bradley W. Peterson, *Final HIPAA Privacy Rules: "How Do We Get Started?"*, J. HEALTH CARE FIN. (2001); *see also, e.g.*, American Hospital Association Detailed Comments to the DHHS (hereinafter "AHA Detailed Comments"), Mar. 30, 2001; *see also, e.g.*, Amy Snow Landa, *Panel Wants HIPAA Privacy Loophole Closed,* American Medial News, Mar. 25, 2002 (challenging that the Privacy Rule fails to adequately protect patients from commercial marketing activities).

16. 45 C.F.R. § 164.502 (2002).

17. Guidance for the Standards for Privacy of Individually Identifiable Health Information, Office for Civil Rights, July 6, 2001 (hereinafter "Guidance") (updated Jan. 14, 2002). To ensure that the final Privacy Regulations protected patients' privacy without creating unanticipated harmful consequences, Secretary Thompson took

Annals of Health Law, Vol. 12 [2003], Iss. 1, Art. 7

will inevitably vary from case to case, depending upon the particular facts and circumstances involved. As a result, the "minimum necessary" standard will become a significant cost burden and an overall challenge to the goal of full compliance.[18]

Finally, the Notice of Privacy Practices will be discussed. With the final modifications' removal of consent, this notice requirement has received an increased amount of attention. The regulations require covered entities to provide individuals with adequate notice of specific privacy rights and practices.[19] The administrative and cost burdens associated with this notice, however, present a challenge to covered entities. Moreover, subjective language found in the accompanying acknowledgment requirement also leaves entities with little direction for future compliance. Although it was an important initiative to remove the mandatory consent form, the notice section of the Privacy Regulation could benefit from a little more Departmental attention. Future guidance and interpretation are necessary in most areas if covered entities are expected to comply with the regulations by the April 2003 deadline.

II. The Burden of Preemption Analysis

A. A General Look at Preemption

The term "preemption" is a judicial doctrine that originated through interpretation of the Supremacy Clause of the United States Constitution.[20] In effect, the Supremacy Clause stands

public comments on the final rule. During a 30-day comment period in Mar. 2001, HHS received more than 11,000 separate comments on the final rule. In July 2001, HHS issued an initial set of guidance materials to address common misconceptions and provide clarification for the final Privacy Regulations, *available at* http://www.hhs.gov/ocr/hipaa; *see also, generally*, John R. Christiansen, *The First Official Guidance on the HIPAA Privacy Rule: Reality Checks Back In*, The Informatics Review (2001), *available at* http://www.informatics-review.com/thoughts/reality.html.

18. In fact, the "minimum necessary" standard is the second largest cost in complying with the Privacy Regulations. HHS estimates that "the requirement that disclosures of protected health information only involve the minimum amount necessary, [will be] $5.8 billion over ten years." The largest cost item, the requirement to have a privacy official, led by a small margin—$5.9 billion over ten years. Privacy Rule, 65 Fed. Reg. 82,462, 82,760 (Dec. 28, 2000).

19. 45 C.F.R. § 164.520(a)(2002).

20. 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.

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."[21] Such intent may be express or implied. Express preemption exists when Congress explicitly commands that a state law be displaced.[22] On the other hand, under the principles of implied preemption, a state law is displaced "if federal law so thoroughly occupies a legislative field as to make reasonable the inference that Congress left no room for the States to supplement it."[23]

B. The General Preemption Rule and its Exceptions

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 permitted three exceptions to this general rule. First, there is an exception for state laws that the Secretary 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 grant of authority from the Secretary of HHS, called

21. Ill. Ass'n of Mortgage Brokers v. Office of Banks & Real Estate, 174 F. Supp. 2d 815, 823, (N.D. Ill. 2001).

22. Orson, Inc. v. Miramax Film Corp., 189 F.3d 377, 381 (3d Cir. 1999). The Employee Income Retirement and Security Act of 1974 (hereinafter "ERISA"), for example, states that the provisions of the Act "shall supercede any and all State laws insofar as they may now or hereafter relate to any employee benefit plan." 29 U.S.C. § 1144(a)(1994).

23. United States v. Vasquez-Alvarez, 176 F.3d 1294, 1297 (10th Cir. 1999). For a more thorough explanation of preemption, *see also* Marin R. Scordato, *Federal Preemption of State Tort Claims*, 35 U.C. DAVIS L. REV. 1 (2001).

24. 42 U.S.C. § 1320 d-7(a)(1).

25. 45 C.F.R. § 160.202 (2002). *See also* Miramax, *supra* note 22, at 382, which uses similar language to define "conflict."

26. 42 U.S.C. § 1320d-7(a)(2)(A)(i).

27. 42 U.S.C. § 1320d-7(a)(2)(A)(ii).

an "exception determination," in order to be saved from preemption.[28] The Privacy Regulations create a distinct section for this "exception determination" process.[29] 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.[30] Laws that fall under this exception do not need a Secretary determination to avoid being preempted.[31] Unlike the "exception determination" process applicable to the first two exceptions, HHS does not provide any comparable guidance for state laws related to the privacy of individually identifiable health information. Thus, all state laws in this group must be independently analyzed, and those that are more protective of privacy are saved from preemption.[32] This type of analysis is a major drawback for covered entities because they are forced to ascertain the "stringency" of a number of state privacy laws.[33] Those entities that choose to engage in the analysis on their own will find it a

28. *See* 45 C.F.R. §§ 160.203(a), 160.204 (2002).

29. Any contrary state law that may fall into one of the above exceptions may be submitted to the Secretary for a unique preemption determination. The request must be in writing and contain several pieces of necessary information. For example, the request must include the ways in which certain entities would be affected by the exception, the reasons why the state law should not be preempted, and any other information relevant to the Secretary's determination. 45 C.F.R. § 160.204 (2002). After reviewing the information, the Secretary makes a determination as to whether the state law is subject to federal preemption. This determination will ultimately be made "on the basis of the extent to which the information provided [by the requester] and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met." 45 C.F.R. § 160.204(c) (2002). This "criteria" refers to the factors required by the first two exceptions, described above (if the state law is necessary: to prevent fraud and abuse, to ensure appropriate state regulations of insurance and health plans, for state reporting on health care delivery, or for other purposes, or if the state law addresses controlled substances). 45 C.F.R. § 160.203(a) (2002).

30. *See* 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).

31. 45 C.F.R. § 160.204(a) (2002).

32. Some label this a "federal floor" of preemption. In the preemption comment section of the final Privacy Regulations, HHS repeatedly uses this term in its commentary responses. The Department addresses both praises and criticism of the "federal floor" approach. Privacy Rule, 65 Fed. Reg. 82,462, 82,580 (Dec. 28, 2000); *see also* AMA Comment Letter to HHS, dated Mar. 30, 2001 (taking the position that the several exceptions allowed by HIPAA create a "weak" federal floor) (hereinafter "AMA Comment Letter"); *see also* WEDI-SNIP, White Papers, Preemption, Dec. 2001, at 14 (hereinafter "Preemption White Papers") for a "federal floor" discussion; *see also* Christopher C. Gallagher, *Health Information Privacy: The Federal Floor's State Elevator*, Sept. 7, 2001, *at* http://www.gcglaw.com/resources/healthcare/healthprivacy.html.

33. Although this stringency analysis is part of the complex preemption analysis, preemption analysis involves the examination of many other factors.

considerably difficult task requiring a fair amount of legal skill. Thus, since many covered entities will hire experienced legal counsel to perform this analysis, significant costs remain a potential burden.

HHS does attempt to assist in the interpretation of the third preemption exception. Specifically, a state law is "more stringent" if one or more of the following are true:

a. The state law prohibits or further limits the use or disclosure of protected health information, except if the disclosure is required by DHHS to determine a covered entity's compliance or is to the individual who is the subject of the individually identifiable information.
b. 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.
c. The state law provides for more information to be disseminated to the individual regarding use and disclosure of their protected health information.
d. 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.
e. The state law imposes stricter standards for record keeping or accounting of disclosures.
f. The state law strengthens privacy protections for individuals with respect to any other matter.[34]

Though HHS does provide a number of examples to assist covered entities, ultimately the preemption analysis becomes a matter of interpretation.[35] Moreover, covered entities are not given any guidance with regard to specific laws that exist in their state.

34. *See* 45 C.F.R. § 160.202 (2002).

35. *See* Landa, *supra* note 9, regarding the SCMA lawsuit filed against HHS. The SCMA also challenged HIPAA on the grounds that it provides an "impermissibly vague" preemption for states that have already enacted patient privacy legislation. The complaint asked the court to overturn the vague HIPAA provision allowing "more stringent" state laws to stand "because a person of ordinary intelligence is unable to determine whether state privacy protections are 'more stringent' than the HHS privacy regulations." According to the SCMA, this violates the Fifth Amendment guarantee of due process, which requires that a statute give citizens fair notice of the conduct prohibited. *Id.* As noted previously, this suit was dismissed on Aug. 14, 2002, and there are no pending appeals.

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 and regulations.[36] 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.[37] Thus, state reporting acts will continue to remain within the control of state legislatures. 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 of facilities or individuals.[38]

C. *How to Perform a Proper Preemption Analysis*

The analysis to determine which state laws are preempted by HIPAA imposes a significant burden on health care providers who may be justifiably uncertain of the standard to which they will be held. In order to ensure compliance, a provision-by-provision comparison of state and federal requirements, as opposed to an overall comparison, is essential. Such an intricate analysis will require considerable time and resources in order for the entity to come into full HIPAA compliance.

In order to conduct a proper preemption analysis, all state laws must initially be considered. The covered entity will have to determine whether *each* state law: (1) is contrary to the federal regulation, (2) is "carved out" from the preemption regulations, (3) requires an "exception determination" from the Secretary under § 160.203(a), (4) is a privacy law, (5) is "related to" the individual regulations in the federal regulation, and (6) is "more stringent" than the federal regulation.[39] Considering such variables, various perspectives and conflicting opinions are inevitable.[40]

Health plans, health care clearinghouses, and health care providers certainly agree on the importance of privacy protection. They cannot, however, be expected to filter through the

36. Congress did not label these provisions as "exceptions" in the original language of HIPAA. 42 U.S.C. §§ 1320d-7(b), (c); *see also* the preamble discussion where HHS recognizes the intent of Congress to "carve out" these specific areas of state authority; Privacy Rule, 65 Fed. Reg. 82,462, 82,580 (Dec. 28, 2000).

37. 42 U.S.C. § 1320d-7(b).

38. 42 U.S.C. § 1320d-7(c).

39. *See* 45 C.F.R. § 160.203 (2002).

40. *See* Preemption White Papers, *supra* note 32, at 14.

intricate language of HIPAA and engage in a legally complex preemption analysis. Covered entities are typically not equipped with the time or personnel to undergo such a task. Moreover, Congress has set forth an unreasonably short compliance period during which the entities must perform and implement the analysis.[41] Inevitably, these entities will need extensive legal assistance in order to determine the effects of HIPAA. Therefore, the covered entity may avoid the actual analysis, yet the cost burdens of this alternative may be even more daunting.[42]

Covered entities must abide by the correct laws. In some situations, the "correct law" may be the more stringent state statute, or a statute that fits into one of the HIPAA exceptions or carve out provisions; other times, HIPAA will preempt and control. It is up to the covered entities to choose how to perform the analysis, but each entity must have the answers by the April 2003 deadline. The challenge associated with preemption analysis in such a limited time frame is obvious. Below are three possible ways for the preemption burdens to be lessened. These alternatives are approached from state, administrative, and legislative angles.

D. Alternatives

(1) States: Assist in the Analysis

In order to ease some of the burden placed on these covered entities, a representative state association (such as a state hospital association, state SNIP, etc.), the state government, or some other collaborative effort could interpret existing state laws in connection with HIPAA.[43] In Illinois, for example, a task force is being led by Dr. John Lumpkin, Director of the Illinois Department of Public Health ("IDPH").[44] This task force represents a combined state effort to resolve the questions regarding preemption and provide solutions to all affected covered entities. IDPH anticipates that through the work of this talented

41. The compliance date for covered entities is set at Apr. 14, 2003 (Apr. 14, 2004 for small health plans). 45 C.F.R. §§ 164.534(a), (b)(2) (2002).

42. The American Hospital Association (hereinafter "AHA") estimates that $351 million will be spent over a five-year period on this preemption provision alone.

43. *See* AHA Detailed Comments, *supra* note 15.

44. *See* Preemption White Papers, *supra* note 32, at 14.

assembly, covered entities in Illinois will be able to rely on the results of a single formal preemption analysis.[45]

Once each state has completed the preemption analysis according to all relevant state privacy laws, it should seek the guidance of the Secretary of HHS.[46] On a state-by-state basis, HHS could review each interpretation and certify the analyses that are validly completed.[47] It follows that, until a preemption analysis has been certified in each state, no penalties should be imposed on those covered entities that have reasonably attempted to incorporate preemptive analyses into their privacy policies and procedures.[48]

Unfortunately, the "exception determination" process described above is not available for those seeking HHS determination as to whether a state law is "more stringent" than HIPAA.[49] In fact, the final Privacy Regulations do not provide any mechanism for covered entities to determine the differences between state and federal law. The Preamble does, however, point to a potentially helpful research project conducted by Georgetown University in July 1999.[50] Although the study is by no means

45. States have taken varied approaches as to which entity conducts the analysis. In Massachusetts, for example, the Boston Bar Association (hereinafter "BBA") is in the process of analyzing state law in connection with HIPAA; *see* http://www.bostonbar.org/gr/sectionwrk/hipaataskforce.htm for information regarding the Massachusetts task force. Michigan, on the other hand, began the task through efforts of the Michigan Health & Hospital Association (hereinafter "MHA"). The MHA anticipates the assistance of attorneys in completing the preemption analysis; *see* comment letter to HHS written by MHA President Spencer C. Johnson (Mar. 22, 2001), *available at* http://www.mha.org/comment/finalhippacomment.asp.

46. *See* Preemption White Papers, *supra* note 32, at 14; *see also* American Academy of Family Physicians statement (hereinafter "AAFP Statement"), submitted to the HHS Regulatory Advisory Committee, Feb. 27, 2000, *available at* http://www.aafp.org/x2459.xml.

47. It is unclear, at this point, whether the Secretary would be willing to offer post-analysis determinations (not to be confused with "exception determinations" found at Process for Requesting Exception Determinations, 45 C.F.R. § 160.204 (2002) or "advisory opinions" which were proposed, yet deleted in the final rule). This "certification" process is only a suggestion, offered in the AAFP Statement, *supra* note 46.

48. AAFP Statement, *supra* note 46.

49. The process for requesting exception determinations, as described in 45 C.F.R. § 160.204 (2002), is used in conjunction with 45 C.F.R. § 160.203(a), in order to save those laws that promote certain social responsibilities. It is not used to define the phrase "more stringent" in state laws related to the privacy of health information. 45 C.F.R. § 160.203(2)(b). The process also is not used to determine application of the "carve out" provisions.

50. Privacy Rule, 65 Fed. Reg. 82,463-82,464 (Dec. 28, 2000); Joy Pritts et al., Health Privacy Project, Institute For Health Care Research and Policy, Georgetown University, *The State of Health Privacy: An Uneven terrain*, 1999, *available at* http://

exhaustive, researchers conducted a 50-state survey of state laws addressing privacy. The resulting compilation may prove to be a helpful tool in the task of preemption analysis.

(2) HHS: Bring Back the Advisory Opinion

Interestingly, the proposed Privacy Regulations included a formal process for seeking HHS advisory opinions with respect to the preemption of state laws relating to the privacy of individually identifiable health information.[51] This process, however, disappeared in the final Privacy Regulations. Numerous comments were received in support of the advisory opinions, yet HHS decided not to adopt the proposed process. In the Comment Section of the Privacy Regulations, HHS attempts to explain its reasons for the retraction.

First, the Department feared that by allowing for an advisory process, covered entities would assume that the Secretary's opinions "would be dispositive of the issue of whether or not a state law was preempted."[52] Although the advisory opinion would indicate how HHS would resolve the conflict and apply the law, such opinions do not bind the courts. As the label implies, these opinions are merely "advisory." Although most courts would give deference to such opinions, HHS was reluctant to implement a process for which the outcome could not be guaranteed.

Second, HHS claims that issuing advisory opinions related to the privacy of individually identifiable health information would be a non-optimal allocation of Department resources. Thousands of questions were received in public comment regarding interpretation, implications, and various aspects of the proposed regulations. As a result, HHS determined that:

> . . .[T]here is no reason to assume that [advisory opinions] will be the most substantial or urgent of the questions that will most likely need to be addressed. It is our intent to provide as much technical advice and assistance to the regulated community as we can with the resources available. . .[U]pon careful consideration, therefore, we have decided that we will be better able to prioritize our workload and be better able to respond to the most urgent and substantial questions raised to

www.healthprivacy.org. In the proposed regulations, HHS declared, "[w]e consider Georgetown's report the best and most comprehensive examination of state privacy laws currently published." Privacy Rule, 64 Fed. Reg. 60,011 (Nov. 3, 1999).

51. *See* Privacy Rule, 65 Fed Reg. 82,580 (Dec. 28, 2000).

52. *Id.*

the Department, if we do not provide for a formal advisory opinion process on preemption as proposed.[53]

The issues raised by these explanations are certainly valid. However, the advisory process would be an important tool in ascertaining which laws are to be applied in a privacy context. Although HHS is wise to abide by a resource allocation scheme, it fails to recognize the level of priority that advisory opinions deserve. Further, although the Department's advisory opinion is not binding, it would still provide more insight than a covered entity could provide on its own. If all covered entities were advised as to the legal consequences of such an opinion, there would be little mistake as to reliance.

(3) Congress: Full Preemption

Generally speaking, HIPAA provides for preemption of contrary state law. Any state law more stringent than its federal counterpart will be allowed to stand.[54] This "federal floor" has been criticized because it provides no preemptive uniformity.[55] Some states may legislate for greater protection, others states may provide for less protection. Further, certain privacy issues may be more heavily protected by the states than others. Such nuances would be discovered by preemption analysis. On the other hand, the inconsistencies are still a considerable burden to covered entities. In the aftermath of HIPAA, covered entities could be forced to comply with a variety of state laws, as well as the federal requirements.[56] This adoption of two standards could prove even more costly for covered entities.

Perhaps there is a need for a "federal ceiling" instead of a "federal floor." Under a full-preemption approach, HIPAA would become the country's single, comprehensive privacy legis-

53. *Id.*

54. State laws that fall into one of the aforementioned "exceptions" or "carve out" provisions will be allowed to stand as well.

55. *See* Gallagher, *supra* note 32.

56. Adding to the confusion is the fact that many states have adopted or are in the process of reviewing the National Association of Insurance Commissioners (hereinafter "NAIC") Insurance Information and Privacy Protection Model Act. This Act, already adopted by at least nineteen states, touches on many issues addressed in HIPAA. Privacy laws in states that have enacted this as legislation are unlikely to be preempted because the Model Act exceeds HIPAA guidelines. Thus, these states are held to the NAIC/state standard regarding the "stringency" analysis, but are held to the HIPAA standard for all other aspects. This creates an additional compliance burden for health care professionals. Victoria Craig Bunce, *Will Legislatures "Opt-In" to More Medical Privacy Standards?,* ALEC Issue Analysis, July 2001.

lation. Full preemption would allow covered entities to follow one given set of rules. It would eliminate the burden of preemption analysis because there would be no question whether to conform to state or federal law. Further, it would give a sense of conformity to the existing "patchwork" of state privacy laws.[57]

A federal privacy law capable of full preemption would substantially benefit covered entities. In reality, no privacy issues are truly state-specific. A patient in Ohio should have the same privacy rights as a patient in California. Further, the variety of state privacy laws presents a challenge to covered entities that practice in more than one state. Recognizing and abiding by the laws of various states places a considerable burden upon covered entities. If this burden were lifted, more time and energy could be spent improving patient care or implementing other aspects of HIPAA.[58]

Covered entities would also be better protected by one uniform standard of privacy regulation. If such a standard were implemented, a cohesive sense of privacy and a more effective source of protection would exist. Full preemption, however, can only be accomplished by lobbying Congress to change the federal standard; HHS does not have such authority.[59] Considering the language used by Congress in HIPAA, however, the chances for full preemption are not encouraging.

E. Preemption Analysis Conclusion

By next April, covered entities will need to know whether they are expected to follow federal or state law in accordance with the Privacy Regulations. Given that the possibility of full preemption is unlikely, an advisory process seems to be the most favorable and least costly alternative. Although the formal process has been removed from the final rule, HHS should provide some other avenue of guidance. For example, the regulations could be expanded to provide more clarity and explanation sur-

57. According to the comments received by HHS, many plans and providers argued that complete federal preemption of the "patchwork" of state privacy laws is, in fact, needed. Privacy Rule, 65 Fed. Reg. 82,579 (Dec. 28, 2000).

58. For example, covered entities must comply with components of HIPAA besides privacy. Ultimately, there will be rules related to security, transaction, identification, and enforcement standards as well.

59. In the commentary section of the final rules, HHS sympathizes with the difficult reconciliation of state and federal privacy requirements. However, HHS reminds commentators that Congress did not grant the authority for HHS to implement full preemption. "[Full preemption is an argument that needs to be addressed to the Congress, not this Agency." Privacy Rule, 65 Fed. Reg. 82,580 (Dec. 28, 2000).

rounding preemption. Alternatively, HHS could certify those analyses that were properly completed, thereby giving a "seal of approval" to be recognized by the industry.

Nonetheless, a test of state versus federal law is not an easy task. It is a time-consuming and costly endeavor, and one that should not be left solely in the hands of the covered entities. As described above, many entities will ultimately hire a law firm to complete the analysis. Others may follow the findings of a state task force, or some similar entity. In the end, however, preemption analysis is only one step in the process of compliance. If it is determined that federal law applies, an entity must comply with the substantive nature of HIPAA. The following section of this paper deals with the minimum necessary standard, an important substantive aspect of the Privacy Regulations. While this requirement is a crucial component in privacy protection, it is greatly in need of modification and clarification.

III. THE "MINIMUM NECESSARY" STANDARD

A. Introduction

When using or disclosing protected health information, or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.[60] This "minimum necessary" standard attempts to limit the misuse of protected health information and ensure a greater level of privacy for patients.[61] HHS believes that this standard will cause covered entities to assess their privacy practices, give the privacy interests of their patients and enrollees greater attention, and make improvements that otherwise might not be made.[62]

While the intended purposes are of significant concern, however, implementation of the minimum necessary standard will be one of the greatest HIPAA compliance challenges.[63] Many believe that this standard overlaps the existing ethical obligation

60. Uses and Disclosures of Protected Health Information, 45 C.F.R. § 164.502(a)(2)(ii)(b) (2002).

61. For example, HHS was concerned that, without the minimum necessary standard, covered entities may be tempted to disclose an entire medical record when only a few items of information are necessary to avoid the administrative step of extracting or redacting information. Privacy Rule, 67 Fed. Reg. 14,786 (Mar. 27, 2002).

62. Privacy Rule, 67 Fed. Reg. 14,786 (Mar. 27, 2002).

63. Broccolo & Peterson, *supra* note 15, at 9.

of a physician to keep a patient's health information confidential.[64] Further, there is a "gray area" between what is necessary information for medical reasons and what is excessive disclosure in violation of the standard.[65] What is "reasonable" is also highly subjective and compounds the problem of the excessive costs of complying with the rule.[66]

When HHS first introduced this standard in the proposed rules, there was a tremendously negative response from covered entities. Many commentators argued that the proposed standard would be contrary to sound medical practice, increase medical errors, and lead to an increase in liability.[67] They believed that a minimum necessary standard would be unworkable in daily treatment situations.[68] Further, they worried whether such a standard would cause practitioners to withhold information necessary for future treatment.[69] In response to these suggestions, HHS significantly revised the regulations pertaining to the minimum necessary standard. The burdens of its interpretation and application, however, are far from resolved.

B. The General Standard and its Exceptions

Requirements for implementation of the minimum necessary standard can be found in Section 164.514(d) of the Privacy Regulations.[70] This section separates "uses," "disclosures," and "requests" into three distinct categories. For "uses," a covered entity must develop and implement certain policies and procedures that identify: (1) the individuals or classes of individuals within its workforce who need access to protected health information in order to carry out their duties, and (2) the category or categories of protected health information to which such persons or classes need access.[71] These role-based access rules must also identify the conditions, as appropriate, that would apply to such access.[72] For example, certain categories of workers may only be entitled to access protected health information during time periods when they are on duty.[73]

64. AMA Comment Letter, *supra* note 32.
65. *Id.*
66. *Id.*
67. Privacy Rule, 65 Fed. Reg. 82,712 (Dec. 28, 2000).
68. *Id.*
69. *Id.*
70. 45 C.F.R. § 164.514(d) (2002).
71. 45 C.F.R. § 164.514(d)(2)(i)(A)-(B) (2002).
72. Privacy Rule, 65 Fed. Reg. 82,713 (Dec. 28, 2000).
73. Privacy Rule, 65 Fed. Reg. 82,713-82,714 (Dec. 28, 2000).

For "disclosures" and "requests" covered entities must limit the disclosure or request to that "which is reasonably necessary to accomplish the purpose" for which the disclosure or request is made.[74] For routine and recurring disclosures or requests (i.e., billing inquiries), the covered entity must implement policies and procedures that assure this limitation. In all other circumstances, the covered entity must conduct an individual, case-by-case review of the intended disclosure or request.

The minimum necessary standard, however, does not apply to the following:

(1) Disclosures to or requests by a health care provider for treatment,
(2) Uses or disclosures made for which the covered entity has received an authorization,
(3) Uses or disclosures made required for compliance with the standardized HIPAA transactions,
(4) Uses or disclosures to HHS, required for compliance with the Privacy Regulations, and
(5) Uses or disclosures required by law.[75]

These exceptions were included by HHS based on specific policy objectives and significant commentary by affected covered entities. The most significant exception is that for disclosures to or requests by a health provider for treatment. In the proposed regulations, providers who disclosed or requested information for treatment purposes were subject to the minimum necessary requirement. Comments surged into HHS, claiming that this would cause practitioners to withhold information that could be essential for subsequent care.[76] Many argued that caregivers need to be able to give and receive a complete picture of the patient's health to make a diagnosis and develop a treatment plan.[77]

In response to these concerns, HHS developed the exception for provider treatment. Without a doubt, this exception was probably the most necessary and significant addition to the final

74. 45 C.F.R. § 164.514(d)(3)-(4) (2002).

75. 45 C.F.R. § 164.502(b)(2)(i)-(v) (2002). Under these regulations, the standard does not apply to disclosures made to the Secretary of HHS for compliance with HIPAA standardized transactions.

76. Privacy Rule, 65 Fed. Reg. 82,712 (Dec. 28, 2000).

77. Privacy Rule, 65 Fed. Reg. 82,713 (Dec. 28, 2000).

Privacy Regulations.[78] A physician no longer had to endure the burden of ascertaining the minimum necessary amount of information when disclosing or requesting protected health information for treatment purposes. In fact, an entire medical record may be disclosed or requested by a health care provider for purposes of treatment, without fear of violating HIPAA.[79]

C. "Uses" in Treatment Settings

The exception for provider treatment, however, comes with an important caveat. Neither the proposed, nor the final regulations included an exclusion for the "use" of protected health information for treatment purposes.[80] Rather, only provider "disclosures" or "requests" of information are exempt from the minimum necessary requirement. Although HHS has received several comments regarding this omission, it has intentionally neglected to include this important exclusion in the Final Rule.

In order to implement a minimum necessary standard for "uses" of protected health information, an entity must establish policies and procedures identifying individuals (or classes of individuals), and their rights of access to protected health infor-

78. The AMA concludes that this provision "will ensure that physicians have the flexibility to send and receive adequate information and provide patients the treatment they need." AMA Comment Letter, *supra* note 32.

79. The regulations require that an entire medical record may only be disclosed when it is "specifically justified as the amount that is *reasonably* necessary to accomplish the purpose of the use, disclosure, or request." 45 C.F.R. § 164.514(d)(5) (2002). HHS clarifies that "no justification is needed in those instances where the minimum necessary standard does not apply, such as disclosures to or requests by a health care provider for treatment [purposes] . . .."; Guidance, *supra* note 17, at 11.

80. On Aug. 14, 2002, the Department published final modifications of the Privacy Regulations. Privacy Rule, 67 Fed. Reg. 53,182 (Aug. 14, 2002). This much anticipated response will likely be the last set of formal standards released before the Apr. 14, 2003 compliance date. The final modifications were issued subsequent to proposed modifications published on Mar. 27, 2002. Privacy Rule, 67 Fed. Reg. 14,776 (Mar. 27, 2002). During a 30-day comment period, HHS considered public comments on the proposed changes before issuing the final modifications that are currently in place. *See* Press Release, *HHS Issues First Major Protections for Patient Privacy*, U.S. Dep't of Health and Human Service Press Office, Aug. 9, 2002; *see also* Fact Sheet, *Modifications to the Standards for Privacy of Individually Identifiable Health Information – Final Rule*, U.S. Dep't of Health & Human Servs. Press Office, Aug. 9, 2002; *see also* Press Release, *HHS Proposes Changes That Protect Privacy, Access to Care*, U.S. Dep't of Health & Human Servs. Press Office, Mar. 21, 2001; *see also* Fact Sheet, *Protecting the Privacy of Patients' Health Information*, U.S. Dep't of Health & Human Servs. Press Office, Apr. 2, 2002; *see also* Fact Sheet, *Standards for Privacy of Individually Identifiable Health Information – Proposed Rule Modification*, U.S. Dep't of Health & Human Servs. Press Office, Apr. 2, 2002.

mation.[81] In order to give covered entities a better understanding of when information may be "used," several examples of acceptable policies and procedures were provided in the regulatory preamble.[82]

In one example, HHS determined that a hospital policy could allow physicians access to all records, subject to the condition that viewing the records of patients not under their care must be recorded and reviewed (e.g., by a staff member).[83] The problem is that some staff might not be aware of which patients belong to which physicians or might not be present when the doctor reviews a medical record.[84] This could potentially create a problem, particularly in emergency situations when physicians are called upon to treat patients not normally under their care.[85] Under such conditions, it is important that the attending physician has immediate access to all of the patient's medical records, and that the process is not delayed by staff questioning them, or determining which patients are under the physician's care.[86]

In a second HHS illustration, a hospital policy could give nurses access to full patient medical records, but only for patients in the nurse's ward and only during the time the nurse is on duty.[87] This access restriction, however, would be incredibly difficult to implement and may also compromise patient care:

> Patients and nurses are often transferred between wards, which could prevent a nurse access to a patient's chart until the medical record or computer system was updated to reflect the relocation of the patient or the nurse to a different ward. Some nurses monitor a variety of patients based on the patient's condition or supervising physician. Therefore, restrictive policies for nurses may not be appropriate.[88]

---

81. 45 C.F.R. § 164.514(d)(2)(A)-(B) (2002).

82. Examples are found in the relevant preamble and comment sections of the Privacy Regulations.

83. *See, e.g.*, Privacy Rule, 65 Fed. Reg. 82,713 (Dec. 28, 2000).

84. AHA Detailed Comments, *supra* note 15.

85. *Id.*

86. *Id.*

87. *See, e.g.*, Privacy Rule, 65 Fed. Reg. 82,544 (Dec. 28, 2000).

88. AHA Detailed Comments, *supra* note 15; *see also* the American Organization of Nurse Executives Comment Letter to HHS, Mar. 29, 2001 (hereinafter "AONE Comment Letter"), *available at* http://www.aone.org/news/hipaa_comment_ltr.htm. AONE states it has "grave concern" for the "use" aspect of the minimum necessary requirement. "Within the patient care staff, delineating levels of access to the full complement of patient information based on the role of the individual is counterproductive to the safe and efficient delivery of patient care." The AONE Comment

In certain treatment settings, requiring strict policies and procedures for the "use" of protected health information comes with great concern.[89] Every employee in a facility does not need unfettered access to patient information. Providers in close contact with a patient, however, should be allowed access to whatever information they need to perform their duties.[90]

HHS has not changed its stance with regard to these provider "uses" and, in fact, has published minimum commentary on the issue. The Department has noted, however:

> A number of commentators, especially health care providers, also expressed concern that the minimum necessary restrictions on uses within the entity will jeopardize patient care and exacerbate medical errors by impeding access to information necessary for treatment purposes. These commentators urged the Department to expand the treatment exception to cover uses of protected information within the entity.[91]

HHS recognizes that "treatment settings" often require a quick conveyance of medical information in order to assure effective, high quality health care.[92] The Department also is aware that certain permitted communications and behaviors are integral to the smooth functioning of any institution.[93] HHS, however, stands firm on its position:

> The Privacy Rule is not intended to impede access by health care professionals to information necessary for treatment purposes. As the Department explained in its guidance, a covered entity is permitted to develop policies and procedures that allow for the appropriate individuals within the entity to have access to protected health information, including entire medical records, as appropriate, so that those workforce members are able to provide timely and effective treatment.[94]

Letter states that the rule should be revised so that all providers of patient care services within a health care facility have access to the entire medical record.

89. *See* AONE Comment Letter, *supra* note 88.

90. *Id.*

91. Privacy Rule, 67 Fed. Reg. 14,786 (Mar. 27, 2002) (preamble to the proposed modifications). Note that the final modifications also reveal that "some commentators urged that the Department exempt from the minimum necessary standard all uses of protected health information, or at least uses of protected health information for treatment purposes." Privacy Rule, 67 Fed. Reg. 53,196 (Aug. 14, 2002).

92. Guidance, *supra* note 17, at 9.

93. *Id.*

94. *Id.*

This response merely defers to the original requirement of policies and procedures and fails to make the necessary changes to include provider "uses" of information in the actual rule.

HHS intentionally subjects the "uses" of protected health information to the minimum necessary standard. This was not the result of a mere oversight or omission. Despite much public discord, covered entities will be forced to implement policies and procedures that limit access to information in certain treatment settings and regulate the "use" of health information in the most efficient way possible. Not only will this be an obvious burden to covered entities, but it also poses a serious risk to patient care. By restricting "uses" of patient information in accordance with specific policies and procedures, providers will be unable to offer the maximum quality of care. There exists, however, a significant addition to the final modifications that will reduce some of these harsh consequences. Following in Section D is an analysis of "incidental uses and disclosures" included in the final modifications.

D. The "Incidental Use and Disclosure" Solution!

Although "uses" for provider treatment are not exempted from the minimum necessary requirement, HHS has provided an important addition that will ease some of the burden set forth by the minimum necessary standard. The Department has recognized that certain incidental uses and disclosures are inevitable. By covering oral communications and limiting the use of health information to the minimum necessary, the Privacy Regulations raised concerns that routine conversations between doctors and patients, nurses, and others involved in a patient's care may violate the rule.[95] Many commentators worried that sign-in sheets and bedside charts would need to be abolished and, that empty prescription vials would need to be destroyed.[96] Commentators claimed that the oral communication/minimum necessary requirements could stifle essential communication necessary to provide high quality care.[97]

95. Specifically, the comments expressed concern that doctors could not speak with patients in semi-private rooms, or that doctors could not confer at nurses' stations without fear of violating the rule if overheard by a passerby. *See* Fact Sheet, *Modifications to the Standards for Privacy of Individually Identifiable Health Information— Final Rule*, U.S. Dep't of Health & Human Servs. Press Office, Aug. 9, 2002.

96. Privacy Rule, 67 Fed. Reg. 14,785 (Mar. 27, 2002).

97. *Id.*

In response to numerous concerns from various parties, the Department modified the regulations to include the following:

> (1) Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:
>
> * * *
>
> (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of [the minimum necessary standard] and [the reasonable safeguards requirement]. . . ."[98]

Accordingly, there are several situations and instances that are clarified by this amendment, especially for those who work in large and often crowded treatment settings. While HHS has taken a positive step toward easing many fears, the "incidental uses and disclosures" allowance is not an adequate solution. Even though these incidental uses and disclosures are permitted, they may only occur *after* minimum necessary and reasonable safeguard standards are satisfied. Therefore, this added section has not resulted in any change of provider "uses" for treatment purposes. Treating providers are still subject to the minimum necessary standard and must comply with all policies and procedures before any incidental uses are permitted.

E. What are "Reasonable Efforts?"

Another curious aspect of the minimum necessary standard deals with interpretation of a few key phrases. First, the implementation provisions require that covered entities use "reasonable efforts" to limit the uses, disclosures, and requests of protected health information.[99] HHS has recently verified that covered entities are permitted to make their own subjective assessment as to what would be considered "reasonable."[100] Such a determination could only be made after an entity carefully considers the characteristics of its own business and workforce.[101] In addition, HHS advises that this is not a strict

98. 45 C.F.R. § 164.502(a)(1)(2002).

99. 45 C.F.R. § 164.502(b) (2002).

100. Guidance, *supra* note 17, at 9. Moreover, HHS has repeatedly provided that the minimum necessary requirement is "intended to reflect and be consistent with, not override, professional judgment and standards [of the covered entity]." Privacy Rule, 67 Fed. Reg. 14,786 (Mar. 27, 2002); Privacy Rule, 65 Fed. Reg. 82,543-44 (Dec. 28, 2000).

101. Guidance, *supra* note 17, at 9.

standard, and covered entities need not limit uses or disclosures to those that are absolutely needed to serve its purpose.[102]

According to HHS guidance, covered entities are expected to utilize the input of "prudent professionals involved in health care activities when developing policies and procedures that appropriately will limit access to personal health information without sacrificing the quality of care."[103] Further, HHS calls for an approach consistent "with the best practices and guidelines already used by many providers today to limit the unnecessary sharing of medical information."[104]

Through this guidance, HHS actually creates more confusion than assistance. These guidelines indicate that covered entities are not, in fact, free to make an entirely subjective determination as to what is "reasonable." Instead, they must use the input of "prudent professionals," and the prevailing "best practices" in order to ensure compliance. Moreover, the "best practices" approach pushes the standard to a level much higher than that of a "prudent professional." By requiring the "best," HHS suggests that covered entities must go above and beyond the prevailing norms of professional standards. In effect, this guidance holds entities to an almost impossible standard. Some suggest, however, that the "best practices" approach was merely a goal to be reached, and not a requirement to be followed.[105]

Regardless, it is clear that there are external factors that should be considered when developing policies and procedures.[106] HHS will allow covered entities to make a good faith determination, while abiding by certain objective standards and using expert opinion in order to achieve those standards.[107] Until HHS releases more definitive guidance,[108] however, these en-

102. *Id.*

103. *Id.* at 10.

104. *Id.* at 9.

105. Michael L. Blau, *The Minimum Necessary Standard: A Substantial Compliance Challenge*, McDermott, Will & Emery Health Law Department Publications, Oct. 25, 2001, *available at* http://www.mwe.com/health/blaumin.htm.

106. *Id.*

107. *Id.* Comments received by HHS suggested a "good faith" provision to all disclosures subject to the minimum necessary standard in order to mitigate liability for honest violations. In addition to allowing the covered entity to use standard protocols for routine disclosures, HHS responded by stating, "we modify [from the proposed regulations] the proposed standard to require the covered entity to make reasonable efforts [not all reasonable efforts as proposed] to make the minimum necessary standard." Privacy Rule, 65 Fed. Reg. 82,714 (Dec. 28, 2000).

108. Surprisingly, the proposed modifications did not resolve any of the ambiguity surrounding the standard. HHS merely reiterated that the minimum necessary stan-

tities will be forced to comply at a heightened level that was probably never intended.[109]

Second, the Privacy Regulations originally called for a covered entity to reasonably ensure that it met the standards, requirements, and implementation specifications for the minimum necessary standard.[110] Comments have expressed concern that the term "reasonably ensure" connoted an absolute, strict standard, and therefore, was "inconsistent with the Department's intent that the minimum necessary requirements be reasonable and flexible to the unique circumstances of the covered entity."[111]

As a result of this commentary, the term "reasonably ensure" was deleted upon publication of the final modifications. Indirectly, this can be taken as a sign that the Department does not wish to appear authoritarian or exacting in its implementation of the minimum necessary standard. On the contrary, the subjective nature of the standard is apparent and should be applied more readily to the "reasonable efforts" discussion as well. This, however, is not a decision to be made by the covered entities without more definitive guidance from HHS.

F. Minimum Necessary Conclusion

The protective nature of the Privacy Regulations is accomplished through significant provisions such as the minimum necessary standard. To divulge only the minimum necessary amount of protected health information is to give the patient an increased level of privacy protection. While this will remain a great advantage in some regards, it proves quite burdensome to the covered entities that are required to implement the standard.

---

dard is a "reasonableness standard," intended "to be flexible to account for the characteristics of the entity's business and workforce." Privacy Rule, 67 Fed. Reg. 14,785 (Mar. 27, 2002).

109. *See* Blau, *supra* note 105, where the author advises that the "best practices" approach is somewhat misleading. He notes that interpretive guidance is a lower level legal authority than a statue or regulation and, thus, the approach should not be read as legally definitive. Further, the author points out that agency interpretations are entitled to due deference, thus suggesting that the "best practices" approach should be better explained/clarified when HHS issues a guidance update. It is the opinion of this author that the *entire* "reasonableness" standard needs to be better explained/clarified in the next guidance in order to ascertain the Department's true intent.

110. 45 C.F.R. § 164.514(d)(1).

111. Privacy Rule, 67 Fed. Reg. 53,195 (Mar. 27, 2002).

First, HHS needs to expand the provider treatment exception to "uses" of protected health information. To ignore this necessary extension may seriously compromise the provision of adequate patient care. Permission for "incidental uses and disclosures" is a positive, yet deceiving step in the right direction. While many indirect or unintentional uses and disclosures are now permitted, they are dependent upon an *already* permitted use or disclosure. The minimum necessary standard must still be met before any incidental use or disclosure may take place. Second, HHS needs to determine the level of reasonableness required of the covered entities so that policies and procedures may be created. Ultimately, once all necessary modifications and clarifications have been made, the minimum necessary standard should prove to be an effective and extremely integral component of the Privacy Regulations.[112]

IV. The Notice of Privacy Practices

A. *Elimination of Consent*

Arguably, the most significant aspect of the final modifications was the removal of a mandatory consent requirement.[113] After a wavering history,[114] the consent requirement has been eliminated from the Privacy Regulations based on concerns that

112. HHS has recently stated, "[t]he privacy benefits of retaining the minimum necessary standard outweigh the burden involved with implementing the standard." Privacy Rule, 67 Fed. Reg. 53,197 (Mar. 27, 2002).

113. The consent requirement required health care providers who had a direct treatment relationship with an individual to obtain the individual's consent prior to using or disclosing protected health care information for treatment, payment, or health care operations. 45 C.F.R. § 164.506 (2002). For commentary regarding this removal, *see* Privacy Rule, 67 Fed. Reg. 53,208-53,214 (Mar. 27, 2002).

114. The proposed regulations did not provide for any form of consent. Subsequent commentary received by HHS, however, supported the addition of a consent requirement. Privacy Rule, 65 Fed. Reg. 82,648 (Dec. 28, 2000). Many individuals argued that providing consent enhances their control; many advocates argued that the act of consent focuses patient attention on the transaction; and many health care providers argued that obtaining consent is part of ethical behavior. *Id.* These comments argued that consent for treatment, payment, and health care operations was necessary for maintaining the integrity of the health care system. As a result, HHS included a consent requirement in the final Privacy Regulations. *See* 45 C.F.R. § 164.506 (2002). Mainly, this was done in order to encourage physician-patient interaction by giving the individual the "appropriate opportunity to consider the appropriate uses and disclosures of his or her protected health information." Privacy Rule, 65 Fed. Reg. 82,648 (Dec. 28, 2002). Later, the pendulum swung back when the proposed modifications were released in support of the elimination of consent. Privacy Rule, 67 Fed. Reg. 14,182 (Mar. 27, 2002). This proposal was the result of many comments disfavoring consent based on concerns that its inclusion would impede access to, and delivery of, health care. Privacy Rule, 67 Fed. Reg. 14,779 (Mar. 27, 2002). As

significant practical problems would pose obstacles to the timely access to health care.[115] One of the most pervasive consent issues was that providers would not be able to use or disclose protected health information for treatment, payment, or health care operations prior to an initial face-to-face interaction with the patient.[116] Additionally, the consent requirement was seen as an administrative burden and duplicative of the information already contained in the Notice of Privacy Practices.[117] Further, many physicians argued that they already had an ethical obligation to maintain patient confidentiality and typically obtain consent as a matter of course.[118]

The final modifications make the consent process entirely discretionary for covered entities.[119] All covered entities now have the same regulatory permission for routine uses and disclosures such as treatment, payment, or health care operations.[120] Although the removal of such a burdensome requirement will undoubtedly be applauded by covered entities, other administrative hurdles remain. First, elimination of the consent requirement only applies to treatment, payment, and health care

---

it turns out, the final modifications mirrored the proposal and removed consent as a mandatory requirement. Privacy Rule, 67 Fed. Reg. 53,208 (Mar. 27, 2002).

115. Privacy Rule, 67 Fed. Reg. 53,209 (Mar. 27, 2002).

116. *Id.* The preamble lists several specific examples and concerns that would have resulted from inability to use or disclose information prior to a face-to-face encounter. These include: (1) pharmacists would not have be able to fill prescriptions, verify coverage, or determine eligibility before the patient arrived at the pharmacy to pick up the prescription, and (2) hospitals would not have be able to use information from a referring physician to schedule appointments or prepare for a patient visit prior to the patient's arrival for the procedure (or the patient would have had to make a special trip to the hospital to sign the form). *Id.*

117. The consent requirement would have cost an estimated $228 million over the ten-year period from 2003-2012. Privacy Rule, 65 Fed. Reg. 82,761 (Dec. 28, 2000). Removing this duplicative requirement therefore, was a significant cost savings as well.

118. AMA Comment Letter, *supra* note 32. Consent forms are currently a popular device. A 1998 study examined hospital consent forms regarding disclosure of medical information. It found that 97% of all hospitals seek consent for the release of information for payment purposes; 45% seek consent for disclosure for utilization review, peer review, quality assurance, and/or prospective review; and 50% seek consent for disclosure for providers, other health care facilities, or others for continuity of care purposes. All of these activities fall within the definitions of "treatment," "payment," or "health care operations." 65 Fed. Reg. 82,648 (Dec. 28, 2000) (*citing* J. Merz, P. Sankar & S.S. Yoo, *Hospitals Consent for Disclosure of Medical Records*, 26, J.L., MED. & ETHICS, 241, 241-48 (1998).

119. 45 C.F.R. § 164.506(b)(2002) (*permits*, but does not *require*, a covered entity to obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations).

120. Privacy Rule, 67 Fed. Reg. 53,211 (Mar. 27, 2002).

operations. An authorization is still required for all other uses or disclosures of protected health information not otherwise permitted by the Privacy Regulations.[121] The final modifications have revised and greatly simplified the authorization process, yet covered entities will still be required to obtain patient authorization in advance for all non-routine uses and disclosures.[122] Second, the final modifications have removed consent and strengthened the Notice of Privacy Practices ("Notice"). Covered entities are required not only to inform patients of specific privacy rights and practices, but direct treatment providers must also make a good faith effort to obtain a patient's written acknowledgment of Notice. Following in Section B is a closer look at the Notice requirement.

B. The General Notice Requirement

The Notice of Privacy Practices is a broad, encompassing notification which describes: (1) the uses and disclosures that may be made by a covered entity, and (2) an individual's rights and the covered entity's legal duties with respect to protected health information.[123] It sets forth all uses and disclosures of protected health information that a covered entity is permitted or required to make without the patient's written authorization.[124] Beyond a patient's right to this notice, the regulations are broken into two primary sections: (1) content of notice, and (2) provision of notice.[125] The content requirements are fairly specific. For example, one subpart provides that notice must contain "a description, including at least one example, of the types of uses and disclosures that the covered entity is permitted . . . to make for each of the following purposes: treatment, payment, and health care operations."[126] Further, any time there is a revision, copies must be available upon patient request and the posted notice must be changed accordingly.[127]

Covered entities are also required to follow certain requirements regarding provision of the notice. First, notice must be

121. *Id.*
122. *See* Fact Sheet, U.S. Dep't of Health & Human Servs. Press Office, *Modifications to the Standards for Privacy of Individually Identifiable Health Information – Final Rule*, Aug. 9, 2002.
123. 45 C.F.R. § 164.520(a) (2002).
124. 45 C.F.R. § 164.520(b)(1)(ii)(B) (2002).
125. See 45 C.F.R. § 164.520(b)(2002) ("content" section) and § 164.520(c)(2002) ("provision" segment).
126. 45 C.F.R. § 164.520(b)(1)(ii)(A) (2002).
127. 45 C.F.R. § 164.520(c)(2)(iii) (2002).

provided to a patient no later than the first date of service[128], and duplicates must be available at a covered entity's service sites so that a patient may request a copy to take with them.[129] In addition, notice should be posted in a "prominent location" where it is reasonable to expect that patients who come to a covered entity's service area will be able to read it.[130] Perhaps most importantly, health care providers with a direct treatment relationship to the individual must make a "good faith effort" to obtain a written acknowledgment of receipt of the notice.[131] All covered entities must keep a record of the notice sent to patients and document all written acknowledgments and good faith efforts to obtain the acknowledgments.[132]

Overall, the notice requirement serves a distinct and valuable purpose. It allows patients many opportunities to become familiar with important privacy information through a variety of means. Notice should be provided during an initial office visit, available to take home and read, and conveniently posted in areas where the patient will see it. Hopefully, providers will interpret the "prominent location" language of the regulations to include areas like waiting room or examination room walls. This will provide an easier opportunity for patients to become acquainted with the entity's privacy practices.

C. The Trouble with Notice

HHS received much support for strengthening the notice requirement. Comments suggested that Notice was a reasonable and workable alternative to the consent requirement, and the modifications made by the Department were favored.[133] A number of comments supported the flexibility of its language,

128. 45 C.F.R. § 164.520(c)(2) (2002). For those relationships where the health care provider's first encounter with the patient is over the telephone, mailing the notice to the individual satisfies the notice provision requirements no later than the first date of service. Privacy Rule, 67 Fed. Reg. 53,240 (Mar. 27, 2002).

129. 45 C.F.R. § 164.520(c)(2)(ii)(A) (2002).

130. 45 C.F.R. § 164.520(c)(2)(ii)(B) (2002).

131. 45 C.F.R. § 164.520(c)(2)(ii)(2002). The regulations do provide for an exception for emergency treatment situations ("as soon as reasonably practicable after the emergency treatment situation.") *Id.* Moreover, if an individual fails or refuses to acknowledge the notice, assuming that the provider otherwise documented its good faith effort, there is no violation of the Privacy Rule. Privacy Rule, 67 Fed. Reg. 53,239 (Mar. 27, 2002).

132. 45 C.F.R. § 164.520(e).

133. Privacy Rule, 67 Fed. Reg. 53,239 (Mar. 27, 2002).

which allowed covered entities to implement the notice requirements in accordance with their own practices.[134]

Notwithstanding favorable commentary and obvious benefits, the notice requirement will still be an administrative and costly burden to covered entities. Covered entities will need to create and print many individual pages, large copies to hang on walls, acknowledgment forms, or log books for patients to sign. Further, direct treatment providers must make a good faith effort to obtain a patient's acknowledgment with regard to the notice requirement. Although Notice ultimately conveys important and useful information to patients, its distributional requirements might be more of a hassle than that of the previous consent requirement. On the other hand, however, one major benefit is that a covered entity is not required to abide by *both* constraints in order to ensure compliance.

Further, patients might not receive the same benefits with notice requirements as they did with the consent requirement. Notice hanging on a wall or in an examination room does not draw adequate attention to the importance of a covered entity's privacy-protective behaviors. It does not necessarily compel the patient to discuss potential uses or disclosures with his or her provider. And, there is no "initial moment" when patients may raise questions about privacy concerns.[135] A signed acknowledgment does not rise to the same level as a signed consent form. Moreover, a "good faith effort" does not equate to asking a patient whether they have read or understood the material, or if they have questions.[136] Although the burden of consent was fortunately stripped from the Privacy Regulations, the benefits of its significance must be preserved, and the notice requirements must be further strengthened.

Another foreseeable problem with the Notice requirement is the subjective nature of the acknowledgement section. Although HHS created the notice requirements to be flexible and adaptable for all entities (and thus reduce the burden), their leniency may have a negative impact upon patient education of

134. *Id.*

135. The proposed modifications suggested that the strengthening of the notice requirement would preserve a valuable aspect of the consent process in that it would create an "initial moment" between the patient and provider, where the individual could focus on information practices and privacy rights and discuss specific concerns with the provider regarding the privacy of his or her protected health information. Privacy Rule, 67 Fed. Reg. 53,238-39 (Mar. 27, 2002).

136. Privacy Rule, 67 Fed. Reg. 53,239 (Mar. 27, 2002).

privacy practices. For example, since covered entities are provided with discretion to design the acknowledgment process that works best for their businesses, they are free to set up relaxed procedures that could potentially fail to adequately provide patients with privacy information.[137]

In addition, the modifications now require that direct treatment providers make a "good faith effort" to obtain a patient's written acknowledgement of the notice of privacy rights and practices.[138] The only requirement is that the acknowledgment be "in writing" and may include a mere signature on a logbook. For Notices sent through the mail, the provider may include a tear-off sheet or other document that requests such acknowledgment be mailed back to the provider.[139] Even if the patient fails to return the acknowledgment, a good faith effort shields the provider from violation of the Privacy Regulations.[140]

Accordingly, the notice requirements are not heavily burdensome and leave ample room for entities to assimilate the rules into practice. As a result, however, there is a serious risk that patients will not be informed of the privacy rights and practices required by the Rule. Regardless, the notice requirement might still be sufficient if several changes are made. First, HHS should either eliminate the "good faith effort" requirement or provide substantial guidance as to what such an effort entails. Although the preamble suggests that interpretive guidance is on the horizon,[141] covered entities will likely take advantage of the Rule's subjectivity until that time. Second, if providers take the time to confer with each patient and instigate that "initial moment," then the Notice requirement will indeed become a vehicle through which the patient and physician communicate about privacy.

D. Notice Conclusion

HHS has responded to commentary from numerous providers and others who were greatly affected by the burden of the consent by eliminating the requirement all together. In its place, the Notice of Privacy Practices stands as an integral component that provides substantial information to patients. Although the

137. Privacy Rule, 67 Fed. Reg. 53,240 (Mar. 27, 2002).
138. 45 C.F.R. § 164.520(c)(2)(ii)(2002).
139. Privacy Rule, 67 Fed. Reg. 53,240 (Mar. 27, 2002).
140. *Id.*
141. Privacy Rule, 67 Fed. Reg. 53,239 (Mar. 27, 2002).

Notice's flexibility remains a distinct advantage for covered entities, the subjective nature of the acknowledgment process may hinder patient care. Ultimately, if providers do not collect a definitive acknowledgment from each and every patient *and* supplement the notice requirement with sufficient explanation to all individuals, the Rule will not succeed in its goal.

V. CONCLUSION

If the 1990's were the decade of the Internet, the first decade of 2000 may well be considered the decade of privacy.[142] The Privacy Regulations are an extensive, yet integral component to the complete implementation of HIPAA. These regulations, however, cannot exist alone. They must work in conjunction with the other subparts, mandated by Congress in 1996.[143] The following represent the five areas addressed by HIPAA: (1) Transaction Standards,[144] (2) Security Standards,[145] (3) Identification Standards,[146] (4) Privacy Standards[147], and (5) Enforce-

142. David Newkirk, *Impact of Proposed HIPAA Privacy Regulations on Health Providers*, Second Opinion Customer Educational Guide, Fall/Winter 2000, *available at* http://www.ercgroup.com/secondopinion/articles/hipaa.html.

143. *See* AMA Comment Letter, *supra* note 32, which states:

> [i]n previous HIPAA comments we stated that harmonization is an essential component in implementing the HIPAA standards. The AMA believes that an orderly sequence of implementation is necessary for the goals of administrative simplification to be achieved. First and foremost, we believe that federal privacy standards are an essential precursor and foundation for promulgation and implementation of federal security standards.

144. Health Insurance Reform Standard for Electronic Transactions, 65 Fed. Reg. 50,312 (Aug. 17, 2000). The final Transaction Standards were published in the Federal Register on Aug. 17, 2000, and have a final compliance date of Oct. 16, 2002 (Oct. 16, 2003 for small health plans). On Dec. 27, 2001, President Bush signed into law the Administrative Simplification Compliance Act (hereinafter "ASCA"), allowing a one-year extension for those who are not able to transmit electronic transactions in a standardized format by the compliance date. In order to be eligible for an extension under the ASCA, the covered entity must submit a compliance extension plan to HHS no later than Oct. 15, 2002. Administrative Simplification Compliance Act, Pub. L. No. 107-105, 2001 HR 3323 (Dec. 27, 2001). HHS has provided a model compliance extension plan for covered entities that do not wish to submit an original.

145. Security and Electronic Signature Standards, 63 Fed. Reg. 43,242 (Aug. 12, 1998). The proposed Security Standards were published in the Federal Register on Aug. 12, 1998. The comment period ended Oct. 13, 1998.

146. The proposed National Provider Identification Standards were published in the Federal Register on May 7, 1998. The comment period ended July 6, 1998. National Standard Health Care Provider Identifier, 63 Fed. Reg. 25,320 (May 7, 1998). The proposed National Employer Identification Standards were published in the Federal Register on June 16, 1998. The comment period ended Aug. 17, 1998. Health Insurance Reform: National Standard Employer Identification, 63 Fed. Reg. 32,784 (1998). The proposed National Health Plan Identification Standards are still in development. Although HIPAA also called for Individual Identification Standards, HHS

ment Standards.[148] Each component requires a distinct set of accompanying regulations and each will provide its own specific form of protection. For example, health plans, health care clearinghouses, and health care providers will ultimately speak the same language when the Transaction Standards are implemented. The Security Standards will work to ensure the integrity and confidentiality of information. And the Privacy Standards, once complete, will set forth a significant compilation of patient rights.

Over the last six years, however, the subparts' time frames have diverged from one another. The Transaction Regulations, for example, went into effect in 2000 and require compliance by October 2002.[149] The Privacy Regulations did not take effect until 2001, thus pushing compliance to April 2003.[150] Even more indeterminate are the Security[151] and Identification Standards,[152] which have only been published in a proposed form, and the Enforcement Standards, which have yet to be addressed.[153] Covered entities are currently expected to create systems and procedures with little direction as to final requirements they will be expected to follow. All subparts should require the same compliance date. Unfortunately, this is not the case.

The future of HIPAA is contemplated with bittersweet anticipation. The positive effects of legislation are anticipated, but intrusive and burdensome requirements are feared. First, cov-

---

and Congress have indefinitely postponed any effort to develop such standards. Fact Sheet, U.S. Dep't of Health & Human Servs. Press Office, *Administrative Simplification Under HIPAA: National Standards for Transactions, Security and Privacy*, Jan. 22, 2002.

147. Privacy Rule, 65 Fed. Reg. 82,462 (Dec. 28 2000). The final Privacy Standards were published in the Federal Register on Dec. 28, 2000, and have a final compliance date of Apr. 14, 2003 (Apr. 14, 2004 for small health plans).

148. The proposed Enforcement Standards are still in development. Fact Sheet, U.S. Dep't of Health & Human Servs. Press Office, *Administrative Simplification Under HIPAA: National Standards for Transactions, Security and Privacy*, Jan. 22, 2002.

149. Health Insurance Reform, 65 Fed. Reg. 50,312 (Aug. 17, 2000).

150. Privacy Rule, 65 Fed. Reg. 82,642 (Dec. 28, 2000).

151. Carriage of the Transmissions of Digital Television Broadcast Stations, 63 Fed. Reg. 42,342 (Aug. 7, 1998).

152. National Standard Health Care Provider Identifier, 63 Fed. Reg. 25,320 (May 7, 1998).

153. The proposed enforcement standards are still in development. Fact Sheet, *Administrative Simplification Under HIPPAA: National Standards for Transactions, Security and Privacy*, U.S. Dep't of Health & Human Servs. Press Office, Jan. 22, 2002.

ered entities need to know whether they are expected to follow federal or state law. Although Congress attempted to preempt most contrary state law with HIPAA, it allowed for several exceptions. As a result, many state laws are able to slip through and escape preemption by federal law. The problem, however, is that Congress and HHS have given little guidance with respect to situations where these exceptions apply and expect that the covered entities will be able to make this determination. To complete this task, however, requires a great deal of resources. Though many entities will defer to a law firm or a state task force, the entire process carries a sizable price tag.

Next, the minimum necessary standard needs to be significantly modified and clarified before covered entities can be expected to implement compliant policies and procedures. Most significant is the exclusion of provider "uses" of information for treatment purposes. Large entities such as hospitals cannot be expected to prevent provider "use" of information in all circumstances. Further, HHS needs to release a more clear-cut interpretation of what is meant by "reasonable efforts." Recent guidance attempted this clarification and only added confusion. Although the "minimum necessary" standard has considerable potential for the effective protection of privacy, covered entities need better direction in order to adhere to its complex requirements.

Finally, the Notice of Privacy Practices has been strengthened pursuant to release of the Rule's final modifications. Consent has been eliminated due to potential operational/administrative burdens, and notice has taken on a whole new meaning. While HHS has made a good start with this significant modification, a fair amount of guidance remains necessary. The notice requirements were developed so that patients may be better informed of privacy rights and practices. Although covered entities appreciate flexibility and subjectivity, their policies and procedures should prioritize patient education. In this regard, HHS has almost achieved a balance between benefit and burden.

HHS has a significant amount of work in its future. The Notice of Privacy Practices was an essential and necessary replacement for the overly burdensome consent requirement. The Department has succeeded in easing some of the challenges faced by covered entities in this respect. The "minimum necessary" standard, though not fine-tuned to the most effective level, has been given a fair amount of attention by HHS. With a little

more guidance, the standard will be functional to its greatest potential. Preemption analysis, however, has been overlooked throughout the entire modification process and is more deserving of the Department's time in the future. Although there are many more components to the Privacy Regulations, HHS can only give assistance one step at a time.

The solution for all areas of the Privacy Regulations, therefore, is continued guidance. The three segments highlighted in this paper are greatly in need of clarity in order to ensure smooth compliance by next April. The Department has guaranteed that additional guidance and regulatory modifications are on the horizon.[154] It is important to note, however, that we have seen the final set of *formal* modifications. The proposed and final revisions are a positive step, yet HHS must spend considerable time and resources counseling covered entities and answering complex problems posed by the regulations in place. Only then will the industry be given the chance to comply in accordance with the Rule's true purpose.

April 2003 is getting closer and closer, and covered entities are scrambling to comply with many new and complex requirements. Unfortunately, we are faced with the inevitable reality that time is running out. Ideally, the final compliance date should be pushed back so that covered entities may become familiar with the newest wave of final modifications. In the alternative, compliance should be at least suspended until the Department issues extensive guidance and interpretation. There are only eight months between the release of final modifications and the effective compliance date. This short time frame should be expanded so that covered entities may implement policies and procedures that are integral to the extensive regulations. It would also allow for a more effectual, and lasting, source of privacy protection.

154. Guidance, *supra* note 17, the final rule was issued last July 6, 2001 and was the Department's "first" set of informal guidance.