# PARTIAL PREEMPTION UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

GRACE KO*

## I. INTRODUCTION

The landmark Health Insurance Portability and Accountability Act ("HIPAA"), which President Bill Clinton signed into law on August 21, 1996, was enacted in response to advances in information technology and their dramatic impact on the health care industry.[1] Until recently, most medical records were paper-based, but technological developments have made it increasingly efficient to collect, retain, transmit, and exchange health care data.[2] Title II of HIPAA[3] includes the Administrative Simplification provisions, which mandate the promulgation and adoption of national standards for electronic transactions, thereby encouraging the use of electronic data systems.[4]

Electronic data transmission has sped the delivery of care and the processing of claims, improved systems for identifying and treating those at risk for disease, facilitated medical research, and helped to detect fraud and

* Class of 2006, University of Southern California Gould School of Law; B.A. 1998, Brown University. I would like to thank Michael Shapiro for his guidance and advice.

1. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,465 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160 & 164).

2. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,465.

3. HIPAA also includes the Title I Health Insurance Reform provisions, which were designed to protect health insurance coverage for workers and their families when they lost or changed jobs. *See* HIPAA § 1; Centers for Medicare & Medicaid Services, Overview, http://www.cms.hhs.gov/HIPAA GenInfo/ (last visited Feb. 8, 2006).

4. HIPAA § 261. *See also* Centers for Medicare & Medicaid Services, *supra* note 3.

abuse.[5] But at the same time, by reducing the logistical obstacles to dissemination that had previously helped to preserve the confidentiality of hard-copy records, shifting from paper-based to electronic information systems has increased the risk that sensitive information may become vulnerable to inappropriate uses and disclosures.[6]

Consequently, with the shift to electronic data management, there has been a concomitant increase in concerns about the confidentiality and privacy of medical information.[7] These concerns have been compounded by changes in the health care delivery system, including the rise in integrated and managed-care networks, which have resulted in more entities maintaining and exchanging information. Increasing numbers of individuals and organizations, including some not even affiliated with physicians or health plans, now have access to medical records.[8]

Congress recognized that these changes posed a threat to the longstanding tradition of protecting patient privacy[9] and responded by mandating, in Title II of HIPAA, the promulgation of national, substantive standards to protect patient confidentiality and privacy.[10] Prior to the enactment of HIPAA, the absence of national standards regarding confidentiality hampered efforts to safeguard privacy. Consumers, and the health plans and providers seeking to protect them, were forced to rely on a patchwork of uneven, incomplete, and often inconsistent state laws,

5. HIPAA § 261.

6. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,919–20 (Nov. 3, 1999). In many cases, medical records are kept in databases that can be easily transmitted. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,465–66.

7. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,465–66.

8. *Id.*

9. *See id.* at 82,469 (explaining that Congress recognized "the challenges to the confidentiality of health information presented by the increasing complexity of the health care industry, and by advances in health information systems technology and communications"). *See also* Charity Scott, *Is Too Much Privacy Bad for Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy*, 17 GA. ST. U. L. REV. 481, 491–92 (2000) (arguing that "Americans feel a strong sense of entitlement to health care privacy" and that the ethical foundations of the right to privacy date as far back as the Hippocratic Oath). *Cf.* Joy L. Pritts, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POL'Y L. & ETHICS 327, 328 (2002) (noting that the Hippocratic Oath and other ethical obligations to protect patient privacy were premised on a one-on-one doctor-patient relationship and therefore do not "address the complexities of the modern practice of health care").

10. HIPAA § 264; Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,462.

regulations, and common law.[11] But rather than preempting state law entirely and thereby clarifying the measures that health care entities must take to ensure the privacy of their data, the new privacy standards only partially preempt state law, creating confusion over what law—federal or state—actually governs in particular situations.[12]

When it enacted HIPAA, Congress delegated the responsibility for developing privacy standards to the Department of Health and Human Services ("HHS"), mandating that HHS provide "detailed recommendations on standards with respect to the privacy of individually identifiable health information" within twelve months of HIPAA's enactment.[13] HIPAA further provided that if Congress failed to act on the HHS recommendations within thirty-six months of HIPAA's enactment, responsibility would fall on the Secretary of HHS to promulgate final privacy regulations.[14]

Congress defaulted on its self-imposed deadline, forcing HHS to take the lead in developing privacy standards.[15] The question of federal

11. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 59,920; Rebecca H. Bishop, Note, *The Final Patient Privacy Regulations Under the Health Insurance Portability and Accountability Act—Promoting Patient Privacy or Public Confusion?*, 37 GA. L. REV. 723, 740–41 (2003). *See generally* JOY PRITTS ET AL., GEORGETOWN UNIV. INST. FOR HEALTH CARE RESEARCH & POLICY, THE STATE OF HEALTH PRIVACY: A SURVEY OF STATE HEALTH PRIVACY STATUTES (2d ed. 2003), *available at* http://hpi.georgetown.edu/privacy/publications.html (surveying state statutes that address the use and disclosure of information in the context of providing and paying for health care, but not including regulations, common law, and more generally applicable privacy statutes).

12. *See Interplay Between HIPAA and State Law Uncertain*, PRIVACY FOCUS (Wiley Rein & Fielding, Wash., D.C.), June 2004, at 4, 4, *available at* http://www.wrf.com/docs/newsletter_issues/139.pdf (noting that with regard to HIPAA's privacy provisions, "few issues have engendered as much consistent confusion as the interplay of the [federal] Privacy Rule and state privacy laws"). *See also Privacy Standards: Issues in HHS' Proposed Rule on Confidentiality of Personal Health Information: Hearing Before the S. Comm. on Health, Education, Labor, and Pensions*, 106th Cong. 9–10 (2000) [hereinafter *Privacy Standards Hearing*] (statement of Janet Heinrich, Associate Director, Health Financing and Public Health Issues) (reporting that, of the forty stakeholder groups interviewed about HHS's proposed Privacy Rule, thirty-four raised the preemption provisions in their comments).

13. HIPAA § 264. In developing these standards, HHS was charged with addressing, at a minimum "(1) the rights that an individual who is a subject of individually identifiable health information should have, (2) the procedures that should be established for the exercise of such rights, and (3) the uses and disclosures of such information that should be authorized or required." *Id.*

14. *Id.*

15. *See, e.g.*, S.C. Med. Ass'n v. Thompson, 327 F.3d 346, 348–49 (4th Cir. 2003) (describing Congress's delegation of authority to HHS). This delegation of power has generated some controversy. After HHS enacted the final rule, the South Carolina Medical Association and several individual health care providers filed suit, arguing that Congress had impermissibly delegated its legislative function to HHS. The Fourth Circuit rejected this claim, reasoning that because the HIPAA provisions "provide[d] a general policy, describe[d] the agency in charge of applying that policy, and set boundaries for the reach of that agency's authority," HIPAA provided a comprehensible principle for HHS to follow in its

preemption was one of several intractable policy issues that prevented Congress from passing its own privacy legislation, thus forcing it to default to HHS instead.[16] In November 1999, HHS issued a proposed rule,[17] which generated more than 52,000 public comments.[18] In December 2000, HHS issued its final "Standards for Privacy of Individually Identifiable Health Information," generally referred to as the Privacy Rule.[19] The Privacy Rule was subsequently revised in August 2002.[20] The HHS Office for Civil Rights ("OCR") was charged with general administration and enforcement of the privacy standards.[21]

On the whole, the Privacy Rule has been applauded as a necessary and positive development,[22] although it has faced some broad attacks by stakeholders.[23] The Privacy Rule's preemption provision, however, has

rulemaking. *Id.* at 351. HIPAA and the Privacy Rule thus survived the constitutional challenge on delegation grounds. *Id.* at 351–52.

16. *See* Scott, *supra* note 9, at 513.

17. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (Nov. 3, 1999).

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

19. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000).

20. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,182. Most health care entities subject to HIPAA, such as health plans and health care providers, were required to comply with the Privacy Rule by April 14, 2003. 45 C.F.R. § 164.534 (2005). Small health plans (those with annual receipts of $5 million or less), however, were granted an additional year to comply. *Id.* §§ 160.103, 164.534. The categories of entities subject to HIPAA, known as "covered entities," are enumerated and discussed at length *infra* note 30 and accompanying text.

21. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,472 (noting that the Secretary of Health and Human Services delegated responsibility for enforcement of the Privacy Rule to OCR). *Cf.* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, § 1176, 110 Stat. 1936, 2028–29 (codified as amended in 42 U.S.C. § 1320d-5 (2000)) (granting the Secretary of HHS the power to levy fines for noncompliance with the privacy regulations). In addition, the Department of Justice was charged with investigating criminal violations. *HIPAA Privacy One Year Out: Developments and Lessons Learned*, HEALTH CARE DEP'T ADVISORY (Wiggin & Dana LLP, New Haven, Conn.), June 2004, at 1, 1–2, *available at* http://www.wiggin.com/db30/cgi-bin/pubs/HIPAA%20privacy%20one%20year%20out.pdf [hereinafter *HIPAA Privacy One Year Out*].

22. *See Privacy Standards Hearing*, *supra* note 12, at 9 (reporting "widespread support for the goal of protecting individually identifiable health information from misuse" and noting that, for interested parties, "the issue is not whether to protect medical records privacy but what is the best approach for achieving it"). *Cf.* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,471–72 (noting that "the large number of comments from individuals and groups representing individuals [about the proposed rule] demonstrate [sic] the deep public concern about the need to protect the privacy of individually identifiable health information," but also listing comments that challenged specific provisions of the Privacy Rule).

23. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,588–90 (noting that some public comments to the proposed Privacy Rule challenged its constitutionality on various grounds, including the Commerce Clause, the nondelegation doctrine, separation of powers, and the First, Fourth, Fifth, Ninth, and Tenth Amendments). One group of

created considerable confusion and expense for covered entities.[24] The preemption provision states that HIPAA and any implementing regulations promulgated under its authority preempt contrary state laws.[25] It does not, however, provide for complete federal preemption of all such laws. Rather, it grants a number of express exceptions under which state laws will not be preempted.[26] The definition and application of these exceptions has generated a great deal of confusion and controversy. The partial preemption framework has been criticized as "vague and confusing,"[27] "abstruse and unworkable,"[28] and burdensome, with the potential to "create a compliance nightmare for which no obvious answers exist."[29]

This Note will explore the interaction between the Privacy Rule and state privacy regulations under the partial preemption framework established in HIPAA. Part II explains the statutory and regulatory framework under which preemption analyses are conducted. Part III examines problems raised by the uncertainty of the preemption doctrine's scope, beginning with a discussion of the burdens and obstacles that covered entities face in complying with the preemption provisions. By scrutinizing recent judicial decisions, Part III will show that judges lack a uniform approach for interpreting and applying the rules. Part IV then responds to stakeholders who argue for complete federal preemption of state laws, by demonstrating that partial preemption offers the optimal balance of innovation and uniformity, while also preserving states' rights. Finally, Part V will suggest several ways in which federal and state action can help facilitate compliance and reduce confusion and uncertainty. It argues that Congress should clarify its intent with regard to certain broad preemption questions, and that HHS and states should work together to create state-by-state preemption analyses that both HIPAA-covered entities and enforcement officials can rely on.

physicians and other stakeholders filed suit against HHS, alleging that the Privacy Rule violated its rights under the First, Fourth, and Tenth Amendments. A district court dismissed these constitutional claims, however, reasoning that they were not ripe for judicial review and that the plaintiffs lacked standing to pursue such claims. *See* Ass'n of Am. Physicians & Surgeons v. U.S. Dep't of Health & Human Servs., 224 F. Supp. 2d 1115 (S.D. Tex. 2002), *aff'd* 67 F. App'x 253 (5th Cir. 2003).

24. The Privacy Rule affects a broad range of constituencies, including not only entities bound by its requirements, but also patient advocates, government organizations, and employer and labor groups. *See Privacy Standards Hearing*, *supra* note 12, at 9.

25. 42 U.S.C. § 1320d-7(a)(1) (2000).

26. *Id.* § 1320d-7(a)(2)–(c).

27. *Privacy Standards Hearing*, *supra* note 12, at 12.

28. Sarah Beatty Ratner, *HIPAA's Preemption Provision: Doomed Cooperative Federalism*, 35 J. HEALTH L. 523, 524 (2002).

29. *Id.* at 536.

## II. THE STATUTORY AND REGULATORY FRAMEWORK FOR ANALYSIS

An analysis of the Privacy Law's preemption provision and the problems that it raises necessarily begins with a careful parsing of the statutory and regulatory language. Under the current framework, federal law generally preempts contrary state laws, except under certain express conditions, in which state laws "reverse preempt" HIPAA and therefore control.

The HIPAA requirements apply to any "covered entity," which can be (1) a health plan, (2) a health care clearinghouse, or (3) a "health care provider who transmits any health information in electronic form in connection with" a HIPAA-covered transaction.[30] "Transaction" is defined broadly as "the transmission of information between two parties to carry out financial or administrative activities related to health care."[31] It includes, but is not limited to, the following types of information transmissions: health care claims information, health care payment and remittance advice, health plan eligibility and premium payments, and referral authorization.[32]

The Privacy Rule's preemption provision provides that, with respect to covered entities, federal law "shall supersede any contrary provision of State law."[33] The statutory language mandates a provision-by-provision comparison of federal law and its state counterparts, rather than an overall comparison.[34] Thus, to decide issues of preemption, it is insufficient to determine that a given state law as a whole is either more or less stringent than the corresponding federal law. Instead, the statute demands that individual provisions be compared. Furthermore, "state law" is broadly

30. 45 C.F.R. § 160.103 (2005). The term "health plan" is defined as any individual or group plan that "provides, or pays the cost of, medical care" and explicitly includes a variety of common insurance arrangements, including HMOs, group health plans, and employee welfare benefit plans. *Id.* "Health care clearinghouses" are public or private entities that process health information received from another entity, either from a nonstandard into a standard format or from a standard to a nonstandard format. *Id.* "Health care provider" means a provider of medical or health services or "any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." *Id.* Individual physicians or groups of physicians fall under the definition of "health care provider" and are therefore subject to HIPAA requirements. *See id.*

31. *Id.*

32. *Id.*

33. *See* 42 U.S.C. § 1320d-7(a)(1) (2000).

34. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,582 (Dec. 28, 2000). *See also* 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*, 12 ANNALS HEALTH. L. 143, 152 (2003).

defined to encompass any "constitution, statute, regulation, rule, common law, or other State action having the force and effect of law."[35]

A state law provision is "contrary" to federal law if "(1) A covered entity would find it impossible to comply with both the State and federal requirements; or (2) The provision of state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives" of the Privacy Rule.[36] Generally, the relevant HIPAA provision will preempt state laws that meet either of these conditions. The Privacy Rule, however, carves out several categorical exceptions under which state law provisions contrary to federal law will *not* be preempted.[37] The exception responsible for much of the controversy surrounding the Privacy Rule states that contrary federal law provisions control unless the "provision of State law relates to the privacy of individually identifiable health information and is *more stringent* than a standard, requirement, or implementation specification adopted" under HIPAA.[38] According to 45 C.F.R. § 160.203(b), when a state law privacy provision is more stringent than the corresponding federal provision, the state law will reverse preempt the federal law and will therefore control.[39]

This exception applies only to "individually identifiable health information," which is defined as information collected, created, or received by a covered entity that "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."[40] The information must either

35. 45 C.F.R. § 160.202 (2005).

36. *Id.*

37. *See* 42 U.S.C. § 1320d-7(a)(2)–(c) (incorporating preemption provisions enacted in the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, § 264(c)(2), 110 Stat. 1936, 2033–34).

38. 45 C.F.R. § 160.203(b) (2005) (emphasis added). For the original language of the HIPAA legislation, see HIPAA § 264(c)(2), 110 Stat. at 2033–34 (requiring that a federal regulation "shall not supersede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under [HIPAA]"). The other exceptions to federal preemption apply when (1) the state law provision is determined by the HHS Secretary to be necessary for one of the following reasons: to prevent fraud and abuse, to ensure state regulation of insurance and health plans, for state reporting on health care delivery or costs, or for the purposes of serving "a compelling need related to public health, safety, or welfare"; (2) the state law provides for the reporting of disease or injury, child abuse, birth or death, or is otherwise related to the conduct of public health surveillance, investigation or intervention; or (3) the state law imposes requirements on health plans to report information related to management or financial audits, program monitoring and evaluation, or licensure and certification. 45 C.F.R. § 160.203(a).

39. 45 C.F.R. § 160.203(b).

40. *Id.* § 160.103.

(1) identify the individual or, (2) provide a "reasonable basis to believe that the information can be used to identify the individual."[41]

Two critical questions for HHS were how to define the phrases "relates to" and "more stringent." The scope of the term "relates to" determines the applicability of the 45 C.F.R. § 160.203(b) exception to particular cases. A broad definition would cover provisions with any relationship to the privacy of individually identifiable health information, no matter how peripheral or remote.[42] HHS, however, determined that Congress intended to protect only state laws that specifically or explicitly regulate privacy, not those which regulate it incidentally.[43] Therefore, according to HHS, "[r]elates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way."[44]

HHS's definition of "more stringent" also had the potential to broaden or restrict the scope of the 45 C.F.R. § 160.203(b) exception. To provide more guidance for compliance efforts, HHS rejected the minimalist approach of defining "more stringent" in vague and general terms like "provides more privacy protection." Instead, HHS provided specific criteria applicable to particular situations.[45] A state law is "more stringent" if it meets at least one of six enumerated criteria: (1) it prohibits a use or disclosure of information under circumstances in which the federal law would permit it; (2) it provides subjects of individually identifiable health information with "greater rights of access or amendment" to their information; (3) it provides a "greater amount of information" to subjects about use, disclosure, rights, or remedies; (4) with respect to the form, substance, or need for legal permission prior to a use or disclosure, it provides requirements that narrow the scope or duration, increase the privacy protections afforded, or reduce the coercive effect of the circumstances surrounding the express legal permission; (5) it provides for more detailed recordkeeping or accounting of disclosures; or (6) "[w]ith

41. *Id.*

42. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,996 (Nov. 3, 1999).

43. *Id.*

44. 45 C.F.R. § 160.202 (2005).

45. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 59,997.

respect to any other matter, [it] provides greater privacy protection" for the subject of the information.[46]

Thus, the Privacy Rule constitutes a federal floor of protection rather than a ceiling, guaranteeing a minimum level of federal protection while allowing more privacy-protective state law provisions to survive preemption.[47] With the relevant terms defined, the analytical framework for conducting a preemption analysis emerges. A covered entity would begin by identifying all state law provisions that affect its privacy policies and practices, decide which of those provisions specifically "relate to" the privacy of individually identifiable health information, and then determine whether they are "contrary" to the corresponding federal standard and, if so, whether they are "more stringent."[48] State law provisions that are more stringent will survive and reverse preempt the federal law, while those that are less stringent will be preempted.

This deceptively simple regulatory framework belies the complexities that entities actually confront in performing the preemption analysis. Part III of this Note will explore some of the challenges that covered entities and judges face in analyzing and interpreting the Privacy Rule's preemption provisions.

## III. THE UNCERTAIN SCOPE OF THE PREEMPTION DOCTRINE

Compliance with the preemption provisions is costly and burdensome for covered entities. Their task is complicated by definitional uncertainties in the Privacy Rule that make it very difficult not only for covered entities, but also for courts to determine when state law is in fact preempted. Recent case law, in which two federal circuit courts reached conflicting decisions on the same issue, demonstrates the need for clarification.

### A. THE CHALLENGES TO COMPLIANCE THAT COVERED ENTITIES FACE

For covered entities, the obstacles to complying with the preemption provisions begin with identifying all relevant state law provisions. With regard to statutes and regulations, the main challenge facing covered

46. 45 C.F.R. § 160.202.

47. *See, e.g.*, Bishop, *supra* note 11, at 726 (noting that HIPAA provides a "floor" of protection, which states can exceed).

48. *See, e.g.*, Christopher C. Gallagher, *HIPAA State Law Preemption*, HEALTHCARE PRIVACY LAW (Gallagher, Callahan & Gartrell, Concord, N.H.), Oct. 2002, at 1, 4–8, *available at* http://www.gcglaw.com/resources/healthcare/preemption.pdf (describing a point-by-point strategy to HIPAA preemption analysis).

entities is that relevant provisions "can be found in nearly every nook and cranny of a state's statutes—in obvious and obscure sections of a state's code, buried in regulations, developed in case law, and detailed in licensing rules."[49] HHS has noted that health privacy provisions can be found in laws applicable to issues as diverse as insurance, worker's compensation, public health, birth and death records, adoptions, education, and welfare.[50] At one point, for example, Georgia had over ninety separate statutes affecting health care privacy, and that count did not include case law or state regulations.[51]

This confusion is the legacy of the piecemeal and ad hoc development of state privacy law.[52] In surveying the pre-HIPAA landscape, one author noted that "[p]atient privacy regulations are everywhere and the patchwork character of the law is stunning."[53] Few states have addressed medical privacy by passing a single, comprehensive piece of legislation.[54] Instead, individual health privacy laws have been enacted over time, often in response to "a particular issue which attracts enough public attention for state legislators to be called on to 'do something.'"[55] States have also tended to regulate the diverse users of health information—such as physicians, hospitals, schools, insurers, pharmacies, and researchers—in separate laws.[56] Finally, many laws have been enacted to address specific medical conditions that are especially sensitive or have particularly severe socioeconomic consequences, such as HIV/AIDS, substance abuse, and mental illness.[57]

Because covered entities must respect the laws of the states in which they do business, they have been grappling with this patchwork regulatory system since long before HIPAA's enactment. Therefore, to some extent,

49. JOY PRITTS ET AL., GEORGETOWN UNIV. INST. FOR HEALTH CARE RESEARCH & POLICY, THE STATE OF HEALTH PRIVACY: AN UNEVEN TERRAIN: A COMPREHENSIVE SURVEY OF STATE HEALTH PRIVACY STATUTES (1999) executive summary.

50. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60,005.

51. Scott, *supra* note 9, at 505–06.

52. *See* PRITTS ET AL., *supra* note 11, at ii–iii; Pritts, *supra* note 9, at 333; Scott, *supra* note 9, at 506.

53. Bishop, *supra* note 11, at 740–41.

54. *See* Pritts, *supra* note 9, at 333; Scott, *supra* note 9, at 506. *See also* PRITTS ET AL., *supra* note 11, *passim* (summarizing state privacy laws and demonstrating, state-by-state, that few states have a single comprehensive privacy statute for health information).

55. Scott, *supra* note 9, at 506–07.

56. *See* PRITTS ET AL., *supra* note 11, at ii–iv; Pritts, *supra* note 9, at 333; Scott, *supra* note 9, at 506.

57. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 60,012 (Nov. 3, 1999); Pritts, *supra* note 9, at 335.

entities should already know which state laws apply to them.[58] Nevertheless, the level of familiarity with state law that is required for an entity to conduct a provision-by-provision preemption analysis may be greater than that which is required for it to conduct its day-to-day operations. Preemption analysis may require covered entities to cultivate a greater depth and breadth of knowledge about state law than they needed prior to HIPAA. The task of identifying every applicable state law provision is extremely burdensome on its own. And HIPAA adds yet another layer of analysis, not only by imposing its own set of regulations, but also by forcing covered entities to examine the *interactions* between the preexisting state laws and the new federal standards.[59]

The broad definition of "state law" further complicates the task; it encompasses not only state statutes and regulations, but also constitutions, rules, common law, and any "other State action having the force and effect of law."[60] For example, HHS has made it clear that under some circumstances even local law provisions such as the New York City Code can have the force of state law.[61] Such provisions must then be factored into the preemption analysis. The scope of the preemption analysis thus extends well beyond state statutes and regulations to other sources of potentially relevant law.

Although the preemption framework seems to entail comparing only state law provisions and the corresponding HIPAA standards, covered entities must also consider the impact of other federal laws that affect health privacy, and implicitly factor them into their preemption analyses. In the preamble to the proposed rule, HHS noted that its proposal "would affect various federal programs" and cautioned that some "may have requirements that are, or appear to be, inconsistent with the requirements proposed below."[62] A partial list of federal laws that might interact with the HIPAA standards includes: the Privacy Act of 1974, the Substance Abuse Confidentiality Statute, rules regarding the protection of human subjects in

58. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,581 (Dec. 28, 2000).

59. *See Making Patient Privacy a Reality: Does the Final HHS Regulation Get the Job Done? Hearing Before the S. Comm. on Health, Education, Labor, and Pensions*, 107th Cong. (2001) [hereinafter *Final HHS Regulation Hearing*] (statement of Leslie G. Aronovitz, Director, Health Care Program Administration and Integrity Issues).

60. 45 C.F.R. § 160.202 (2005).

61. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,581 (stating that "to the extent a state treats local law as substituting for state law it could be considered to be 'state law' for purposes of [preemption analysis]").

62. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 59,999.

medical research, the Employee Retirement Income Security Act,[63] the Americans with Disabilities Act, the Family and Medical Leave Act, and Occupational Safety and Health Administration regulations.[64] Additionally, in the litigation context, the Privacy Rule interacts with the Federal Rules of Evidence and the constitutions of individual states.[65]

Preemption analysis thus requires covered entities to identify every possibly relevant regulation across not only the state system, but also the entire set of federal and state laws, from virtually any source, that purports to regulate medical privacy. At a minimum, they must examine the HIPAA standards, state law privacy statutes, administrative rules, common law, federal laws, and even "developing legal theories and . . . international regulations [that may] affect a covered entities' [sic] operations."[66] Then, after the potentially relevant state law provisions are identified, they must be matched to the appropriate federal provisions. This is difficult because the state law provisions do not neatly correspond to federal laws and are not structured in a way that facilitates provision-by-provision comparison.[67]

Many covered entities lack the time, personnel, and technical expertise required to sift through the regulations and conduct their own analyses, so they may instead be forced to seek extensive and costly legal assistance.[68] A survey conducted by the California HealthCare Foundation found that only nineteen percent of respondents planned to perform the analyses in house; the rest planned either to retain external legal counsel or consultants, or to rely on professional industry organizations, state officials, or HHS.[69] Entities that provide services in multiple states—such as health information

63. *See id.* at 59,999–60,001.

64. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,591–92.

65. *Interplay Between HIPAA and State Law Uncertain*, *supra* note 12, at 4–6.

66. WORKGROUP FOR ELEC. DATA INTERCHANGE, PREEMPTION WHITE PAPER 8–9 (2003), *available at* http://www.wedi.org/cmsUploads/pdfUpload/WhitePaper/pub/P-Final-Preemption.pdf [hereinafter WHITE PAPER]. As an example of a potentially relevant "developing legal theory," the Workgroup discusses recent jurisprudence that has overturned state attempts to regulate e-commerce and internet use on Commerce Clause grounds. Further exploration of these developments is beyond the scope of this Note, but the Workgroup cautions that these decisions may affect preemption analyses with respect to transactions that occur across state lines. *Id.* at 11–12.

67. Ratner, *supra* note 28, at 541.

68. *See* Guthrie, *supra* note 34, at 152–53 & n.42 (citing an American Hospital Association estimate that hospitals will spend $351 million over a five-year period to comply with the preemption provision).

69. NAT'L COMM. FOR QUALITY ASSURANCE & GEORGETOWN UNIV. HEALTH PRIVACY PROJECT, CALIFORNIA HIPAA PRIVACY IMPLEMENTATION SURVEY 19 (2002), *available at* http://www.chcf.org/documents/ihealth/HIPAAImplementationSurveyFullReport.pdf.

management groups, hospitals, health plans, and employer groups—face additional costs and administrative burdens because of their need to conduct a separate analysis for each state in which they operate.[70]

While completed preemption analyses are commercially available from various sources, their utility is limited, largely because they do not constitute legal advice and have no force of law.[71] These analyses were created without guidance from the agencies charged with enforcing the Privacy Rule, and therefore do not immunize covered entities from potential liability for noncompliance. These sources also have different levels of credibility. A covered entity may have a difficult time deciding which source to use or how to reconcile conflicting information.[72] In addition, analyses are not available for all states[73] and often apply to only one type of covered entity, such as hospitals or health plans.[74] Another

70. WHITE PAPER, *supra* note 66, at 13. *See also* Bishop, *supra* note 11, at 744 (stating that this problem makes it "onerous, if not impossible, to sell and deliver a uniform [interstate] health plan").

71. *See, e.g.*, 50 State HIPAA Privacy Study, Disclaimer, http://www.statehipaastudy.com/page.aspx?navid=150&catID=399 (last visited Feb. 3, 2006) (advising users that the website's contents are not legal advice and that users should consult legal counsel regarding their particular circumstances).

72. For example, a quick internet search reveals several analyses, ranging in credibility and comprehensiveness, which purport to examine California state laws for preemption purposes. *See* David Humiston & Stephen M. Crane, *Will Your State's Privacy Law Be Superseded by HIPAA?*, MANAGED CARE, May 2002, at 24H, 24H–J, *available at* http://www.managedcaremag.com/archives/0205/0205.hipaabystate.pdf (providing a short and extremely general comparison between California privacy laws and the HIPAA standards); 50 State HIPAA Privacy Study, FAQ, http://www.statehipaastudy.com/page.aspx?navid=130&catID=395 (last visited Feb. 8, 2006); California Hospital Association, Publications, The California Patient Privacy Manual, http://www.calhealth.org/public/pubs/gms/privacy.html (last visited Feb. 8, 2006) (providing ordering information for the *California Patient Privacy Manual*, which includes a preemption analysis); California Office of HIPAA Implementation—Legal Issues, http://www.ohi.ca.gov/state/calohi/ohiGeneral.jsp?sCat=/Nav/Legal%20Issues (last visited Feb. 8, 2006) (offering completed preemption analyses for selected California privacy statutes); National Association of Chain Drugstores Foundation, The HIPAA Preemption Analysis of State Privacy and Security Laws, http://www.nacdsfoundation.org/wmspage.cfm?parm1=91 (last visited Feb. 8, 2006) (providing a chart summarizing state law provisions, listing California as one of the states for which a general preemption analysis, targeted to pharmacists, is available).

73. For example, the 50 State HIPAA Privacy Study website—with legal analysis conducted by Reed Smith LLP and funded by leading health organizations—while probably one of the most comprehensive and complete of the commercial analyses, offered analyses for only forty-one states and jurisdictions as of the April 14, 2003 compliance deadline. 50 State HIPAA Privacy Study, *supra* note 72.

74. *See, e.g.*, National Association of Chain Drugstores Foundation, HIPAA Preemption Background, http://www.nacdsfoundation.org/wmspage.cfm?parm1=74# (last visited Feb. 8, 2006) (providing pharmacy-specific preemption analyses). *See also* WHITE PAPER, *supra* note 66, at 14 (noting that "a bit of due diligence" is required before purchasing a preemption study because such studies are often industry-specific).

problem is that many, though not all,[75] analyses may be prohibitively expensive to obtain, especially for small entities, such as solo practitioners, or for those that need access to information from multiple states.[76]

Additionally, these preexisting analyses may be incomplete because they fail to survey all of the sources of potentially relevant state law. For example, although one major study charges a $20,000 "basic subscription" rate, this fee would not buy a subscriber all of the requisite information because the analysis fails to include local or municipal laws, common law, case law developments, or federal rules and regulations.[77] Furthermore, a preemption analysis cannot be conducted in a vacuum, without considering an individual entity's particular needs and circumstances.[78] Therefore, while available commercial analyses may assist covered entities with their compliance efforts, they do not provide complete solutions to the administrative nightmare that HIPAA's preemption provision creates.

Another problem is that the law is not static—both state law and the HIPAA rules will continually change.[79] States will likely legislate in response to HIPAA, passing new statutes that are "more stringent" than the federal regulations in order to maintain their dominance in the privacy arena. As a result, covered entities will have to "constantly reevaluate the changing state law terrain for each problem."[80] To the extent that the law keeps shifting, so too will the outcomes of preemption analyses—covered entities will not be able to confidently rely on previous assessments. Although the need to monitor changes in federal and state law antedates HIPAA, a new challenge now emerges that requires entities to continually monitor the interaction between the respective reach of these changes. It will be demanding for entities to maintain current preemption analyses.

75. For example, a preemption analysis prepared by the California Hospital Association is available for the relatively low price of $175 for members and $375 for nonmembers. *See* California Hospital Association, *supra* note 72.

76. *See, e.g.*, 50 State HIPAA Privacy Study, How to Subscribe, http://www.statehipaastudy.com/page.aspx?navid=145&catID=398 (last visited Feb. 8, 2006) (charging either $20,000 for a "basic subscription" that allows a single organization access to the entire study or $5000 to $10,000 for an individual state analysis, plus "nominal" annual update charges of about $3000 with either subscription option).

77. *See* 50 State HIPAA Privacy Study, Scope of Study, http://www.statehipaastudy.com/page.aspx?navid=115&catID=393 (last visited Feb. 8, 2006).

78. *Cf.* National Association of Chain Drugstores Foundation, *supra* note 72 (stating that "the applicability or inapplicability of a particular standard depends upon the precise factual circumstances").

79. *See* STEPHEN A. STUART, CAL. OFFICE OF HIPAA IMPLEMENTATION, HIPAA / STATE LAW PREEMPTION FACT SHEET (2003), *available at* http://www.ohi.ca.gov/calohi/docs/Preemption_Factsheet.pdf.

80. Ratner, *supra* note 28, at 545.

The stakes of noncompliance are high. OCR is authorized to impose civil monetary penalties for violations.[81] For entities that "knowingly" violate the Privacy Rule, OCR is also empowered to make referrals for criminal prosecution to the Department of Justice.[82] Criminal violations are potentially punishable by fines or imprisonment.[83] Anyone who believes that a covered entity has violated the Privacy Rule can file a written complaint with OCR, which is then charged with investigating the allegation.[84] OCR has stated its intention to apply a cooperative approach to enforcement, attempting to resolve complaints informally by providing noncompliant entities with the technical assistance necessary to change their practices.[85] Only if such cooperative efforts fail will civil or criminal penalties be imposed.[86] In addition, although OCR is authorized to initiate its own compliance reviews,[87] enforcement efforts will focus on resolving complaints rather than proactively initiating investigations.[88]

Thus, entities may infer that in the event of a complaint, cooperation with OCR will immunize them from liability. There is evidence, however, that this initial phase of cooperative compliance may be only a grace period, and that OCR will soon switch to a tougher enforcement strategy.[89] The agency may have recognized that the regulations are confusing and complicated, and that harsh enforcement from the start would cause panic.[90] Thus, OCR may have considered that it would be more

81. *See* 42 U.S.C. §§ 1320d-5(a)(1), -6(b) (2000) (authorizing a maximum penalty for unintentional violations of $100 per violation, not to exceed $25,000, with increased penalties for willful violations that reach as high as $250,000 and ten years imprisonment in egregious cases).

82. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000).

83. 42 U.S.C. § 1320d-6(b) (authorizing a range of monetary penalties and imprisonment depending on the nature of the violation).

84. 45 C.F.R. § 160.306 (2005). *See also* Fact Sheet: How to File a Health Information Privacy Complaint with the Office for Civil Rights, http://www.hhs.gov/ocr/privacyhowtofile.htm (last visited Feb. 8, 2006) (outlining the procedure for filing complaints).

85. *HIPAA Medical Privacy and Transaction Rules: Overkill or Overdue?: Hearing Before the S. Spec. Comm. on Aging*, 108th Cong. (2003) [hereinafter *Transaction Rules Hearing*] (statement of Richard Campanelli, Director of the Office for Civil Rights, U.S. Department of Health and Human Services).

86. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,472.

87. 45 C.F.R. § 160.308 (2005).

88. *A New Era for HIPAA Enforcement?*, PRIVACY FOCUS (Wiley Rein & Fielding, Wash., D.C.), May 2004, at 3, 3, *available at* http://www.wrf.com/docs/newsletter_issues/125.pdf (noting that OCR has consistently and publicly proclaimed that its enforcement approach will be to "respond to complaints, rather than initiate proactive investigations").

89. *Id.*

90. *See OCR Viewed by Many as "Toothless"; How Aggressively Will It Enforce HIPAA?*, REP. ON PATIENT PRIVACY (Atl. Info. Servs., Inc., Wash., D.C.), June 2004 [hereinafter *OCR Viewed as*

constructive to emphasize education and voluntary compliance during the implementation period.[91] But now that the implementation period is over, OCR has made it clear that it intends to impose civil and even criminal penalties in appropriate cases.[92] Thus far, fifty complaints have been referred to the Department of Justice for potential criminal investigation.[93] Furthermore, OCR retains the power to initiate compliance reviews.

Although bureaucratic delay and scant resources may have initially hampered OCR efforts, the agency received increased funding in fiscal year 2004 and has hired new staff members.[94] One attorney, who previously represented clients against OCR, cautions that "[i]t's time [for OCR] to ramp up. They're getting more serious complaints. It's time for them to levy fines."[95] And another law firm is advising its clients that "[o]n the whole, while covered entities that have been acting diligently to comply with HIPAA's requirements have had 'smooth sailing,' we can expect more aggressive enforcement."[96] In addition, states retain the ability to enforce provisions of their own privacy laws that are not preempted by HIPAA. To the extent that these laws provide private rights of action, covered entities may also face civil suits for committing violations.[97]

*"Toothless"*] (quoting Washington, D.C. attorney Kirk Nahra of Wiley Rein & Fielding LLP as stating that immediate enforcement "would have caused a panic").

91. *See id.* (noting that some practitioners believed that initial enforcement goals were primarily educational).

92. *Transaction Rules Hearing*, *supra* note 85 (quoting Campanelli as stating, "While OCR continues to seek informal resolution through voluntary compliance wherever appropriate, and expects to be able to resolve the vast majority of cases through these informal means, it will employ the variety of enforcement options available as needed . . . ."). *Cf. A New Era for HIPAA Enforcement?*, *supra* note 88, at 3 (quoting Campanelli as stating that a number of cases were "in the pipeline" for both civil and criminal enforcement).

93. *A New Era for HIPAA Enforcement?*, *supra* note 88, at 3.

94. *OCR Viewed as "Toothless,"* *supra* note 90 (quoting New York City attorney Mark Barnes, a private-practice lawyer specializing in HIPAA matters, who claims that budgets and staff hiring have been on the rise).

95. *Id.*

96. *A New Era for HIPAA Enforcement?*, *supra* note 88, at 7.

97. *See* PRITTS ET AL., *supra* note 11, *passim* (describing the remedies available in each state for improper use of privacy information, which include civil suit in many states, such as California, Illinois, Minnesota, Oklahoma, and Texas). *Cf.* Humiston & Crane, *supra* note 72, at 24H (noting that covered entities might face potential liability for making disclosures that are later found to be violations of state law, even if those disclosures were allowed under HIPAA).

## B. THE OPERATIONAL DEFINITIONS OF HIPAA'S TERMS ARE AMBIGUOUS AND INDETERMINATE

A major obstacle to interpreting and applying HIPAA's preemption provision is that much of its language is ambiguous and indefinite. Preemption analysis requires a series of potentially subjective determinations, including whether a provision constitutes "state law" for the purposes of preemption, whether it "relates to the privacy of individually identifiable health information," and whether it is "contrary" to and "more stringent" than the corresponding HIPAA standard.[98] As commentators have noted, such phrases are "inherently difficult to define,"[99] and the fact that their regulatory definitions are not always consistent with a textual, plain-meaning approach[100] makes the analysis even more complicated.

Users may not always have the necessary information to decide how to apply these definitions in a way that is consistent with HHS's intent. For example, a state law provision "relates to" privacy for preemption purposes only if it has the "specific purpose" of protecting privacy or otherwise affects privacy in a "direct, clear, and substantial way."[101] One comment to the proposed rule noted that determining the "specific purpose" of a state law may be difficult or, at the very least, speculative, "because many state laws have incomplete, inaccessible, or non-existent legislative histories."[102] Thus, applying the "relates to" provision requires covered entities to guess at the purpose of state laws, an inferential step that is almost necessarily uncertain.

Other definitional elements of the preemption analysis are equally susceptible to conflicting opinions. The "more stringent" formulation was tested in a recent case. The court evaluated a Louisiana law that does not allow protected information to be disclosed without the patient's consent, unless there is a court order issued after a hearing with the patient "and after a finding by the court that the release of the requested information is

98. *See supra* Part II.

99. Ratner, *supra* note 28, at 526.

100. *Cf.* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,996–98 (Nov. 3, 1999) (elaborating on the definitions of statutory terms).

101. *See* 45 C.F.R. § 160.202 (2005).

102. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,582 (Dec. 28, 2000). HHS was seemingly unconcerned by this issue, and responded that users should be able to ascertain the specific purpose of a state law, "if not from legislative history or a purpose statement, then from the statute viewed as a whole. The same should be true of state regulations or rulings." *Id.* at 82,583.

proper."[103] The corresponding HIPAA standard allows disclosure of protected information without the subject's permission anytime there is a court order, a subpoena, or a discovery request in which the party seeking disclosure made "reasonable efforts" to notify the subject or to secure a qualified protective order.[104] In determining whether the Louisiana provision was more stringent than the HIPAA provision, the court focused on only one of the six criteria given in the statute for making the "more stringent" determination[105] and held that it did not apply to the Louisiana law.[106] The court reasoned that the Louisiana statute did not address the "form, substance, or the need for express legal permission" from the subject because it provided a way of negating the need for express permission by allowing court-mandated disclosure following a hearing.[107] The court thus decided that the Louisiana law did not meet the statutory definition of "more stringent" and, consequently, that the federal law controlled.

Arguably, an equally reasonable interpretation would be that the Louisiana statute was more patient protective and thus more stringent than the corresponding HIPAA provision. The Louisiana law requires both patient participation in a hearing and a judicial finding that the release of the information is proper, prior to disclosure without the patient's consent. HIPAA has neither requirement. Instead, under HIPAA, the party requesting disclosure must merely make "reasonable efforts" to notify the subject in order for information to be released in response to a subpoena or discovery request without the patient's permission.[108]

103. United States *ex rel.* Stewart v. La. Clinic, No. Civ.A. 99-1767, 2002 WL 31819130, at *5 (E.D. La. Dec. 12, 2002) (citing LA. REV. STAT. ANN. § 13:3715.1(B)(5) (2005)).

104. *Id.* at *5–6 (citing 45 C.F.R. § 164.512(e)(1) (2005)). For the definition of a "qualified protective order," see *infra* note 121.

105. A state law is more stringent if, inter alia, the following is true:

> With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, [it] provides requirements that narrow the scope or duration, increase the privacy protections afforded . . . or reduce the coercive effect of the circumstances surrounding the express legal permission.

45 C.F.R. § 160.202.

106. *La. Clinic*, 2002 WL 31819130, at *5.

107. *Id.*

108. *The HIPAA Preemption Mess Continues*, PRIVACY FOCUS (Wiley Rein & Fielding, Wash., D.C.), Oct. 2003, at 3, 3–4, *available at* http://www.wrf.com/docs/newsletter_issues/182.pdf (analyzing *Louisiana Clinic* and the underlying Louisiana statute, LA. REV. STAT. ANN. § 13:3715.1(B)(5) (2005)). A court might decide, for example, that the Louisiana law falls under one of the regulation's other definitions of "more stringent"—for example, that the state law, with respect to any other matter, provides "a more patient-protective provision" than HIPAA. *See id.* (discussing the sixth definition of "more stringent" codified in 45 C.F.R. § 160.202). This argument assumes that the patient can be readily located and will be available to participate in the contradictory hearing. The state law, however,

This case demonstrates that preemption analysis is necessarily indeterminate because many of its definitional elements are ambiguous and susceptible to alternative interpretations. Thus, "[a]s a legal matter, various perspectives will abound and conflicting opinions likely will exist. . . . Even a common understanding of what elements make a statute 'more stringent' will not necessarily be definitive."[109] One practitioner has suggested that the subjective flexibility built into the preemption rule facilitates states' rights in protecting privacy.[110] This is likely of little comfort, however, to the entities that must interpret and apply the definitions in order to comply with HIPAA in their day-to-day operations.

One provider group has challenged the definitional adequacy of the regulations in court.[111] The South Carolina Medical Association alleged that the HIPAA nonpreemption provision, which turns on the definition of "more stringent," is so impermissibly vague that subjecting covered entities to potential fines or incarceration for incorrect determinations constitutes a due process violation.[112] The Fourth Circuit rejected the argument, stating:

> These criteria will doubtless call for covered entities to make some common sense evaluations and comparisons between state and federal laws, but this does not mean they are either vague or constitutionally infirm . . . . [T]he regulations are sufficiently definite to give fair warning as to what will be considered a 'more stringent' state privacy law.[113]

Thus, for the time being, these definitions stand. Unfortunately, "there can be no certainty for practitioners until interpretive decisions begin to shape these terms."[114] The operational uncertainty of the language challenges not only covered entities, but also the courts charged with making these interpretive decisions.

---

may contain provisions allowing for disclosure when the patient cannot, after reasonable efforts, be located. Under these circumstances, the "contradictory hearing" requirement would fall out, and the Louisiana law would be very similar to the HIPAA standard.

109. WHITE PAPER, *supra* note 66, at 17.

110. *See* Gallagher, *supra* note 48, at 2.

111. *See* S.C. Med. Ass'n v. Thompson, 327 F.3d 346 (4th Cir. 2003).

112. *Id.* at 354.

113. *Id.* at 355.

114. Gallagher, *supra* note 48, at 7.

### C. RECENT JUDICIAL DECISIONS DEMONSTRATE THE NEED FOR MORE GUIDANCE AND UNIFORMITY

Thus far, few judicial controversies have implicated the Privacy Rule. Several recent cases, however, have addressed the Privacy Rule's preemption provision in the context of litigation procedures involving evidentiary privileges, discovery requests, and subpoenas.[115] These cases demonstrate that the ambiguity of the preemption provision's language, coupled with a lack of guidance for preemption analysis, will lead judges to make conflicting interpretations and inconsistent decisions.

Two recent cases are especially instructive because they arose from the same underlying dispute—the cases involved the same facts, and yet separate federal courts applied differing preemption analyses to reach opposite conclusions.[116] The underlying substantive suit was the challenge that the National Abortion Federation and physician abortion providers brought against Attorney General John Ashcroft, seeking to challenge the constitutionality of the Partial-Birth Abortion Ban Act of 2003.[117] In each case, the government subpoenaed hospitals to obtain the records of patients on whom the physician plaintiffs had performed certain procedures.[118] The hospitals moved to quash the subpoenas, arguing that, while the HIPAA regulations would permit disclosure under the circumstances, the relevant state laws survived preemption and therefore controlled because they were more stringent and did not permit disclosure.[119]

The HIPAA regulations at issue were the standards governing disclosure of medical information in judicial proceedings.[120] As discussed above, HIPAA regulations allow a covered entity to disclose an individual's health information without written consent in response to either (1) a court order or administrative tribunal order, or (2) a subpoena

115. *See supra* notes 103–04 and accompanying text; *infra* Part III.C. For further discussion of such cases, see *HIPAA Privacy One Year Out*, *supra* note 21, at 2–3.

116. *Interplay Between HIPAA and State Law Uncertain*, *supra* note 12, at 4–6 (analyzing the divergent rulings and judicial rationale that resulted from litigation between the National Abortion Federation and Attorney General Ashcroft—litigation which occurred simultaneously in two different states).

117. *Id. See* Nat'l Abortion Fed'n v. Ashcroft, No. 04C55, 2004 U.S. Dist. LEXIS 1701, at *12 (N.D. Ill. Feb. 5, 2004), *aff'd sub nom.* Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004); Nat'l Abortion Fed'n v. Ashcroft, No. 03 Civ. 8695 (RCC), 2004 U.S. Dist. LEXIS 4530, at *10–11 & n.5 (S.D.N.Y. Mar. 18, 2004), *aff'd sub nom.* Nat'l Abortion Fed'n v. Gonzales, No. 04-5201-CV, 2006 U.S. App. LEXIS 2386 (2d Cir. Jan. 31, 2006).

118. *Interplay Between HIPAA and State Law Uncertain*, *supra* note 12, at 4–6.

119. *Id.*

120. *See id.*

or discovery request not accompanied by court order, as long as the party seeking disclosure makes reasonable efforts to either notify the individual whose information is being disclosed about the disclosure or to secure a qualified protective order.[121] The cases were heard in federal courts in Illinois and New York.

1. The Illinois Rulings

Illinois law prohibits any "healthcare practitioner" from disclosing any information that the practitioner may have acquired in a professional capacity and that is necessary to enable the practitioner professionally to serve the patient, unless one of eleven exceptions applies.[122] It was undisputed that none of the exceptions applied to the facts of the case.[123] Other relevant state law provisions established patients' rights to the privacy and confidentiality of their records,[124] prohibiting hospital medical staff or employees from disclosing information about services provided except to patients or their authorized agents.[125] Thus, the Illinois provisions appear to meet the definition of "more stringent" because they "prohibit[] or restrict[] a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted" under HIPAA.[126]

The court in the Northern District of Illinois applied a straightforward textual analysis, concluding that because the Illinois law prohibited disclosure where HIPAA allowed it, the Illinois provision was "more stringent" and therefore not preempted.[127] The court looked to Federal Rule of Evidence 501, which states that federal common law governs evidentiary privileges unless otherwise provided by an "Act of Congress," and decided that HIPAA was the requisite Act of Congress that supplanted the federal common law.[128] The court held that, because the Illinois provision was activated through HIPAA's antipreemption provision, the state law

121. 45 C.F.R. § 164.512(e)(1) (2005). A "qualified protective order" is an order of a court or an administrative tribunal or a stipulation by the parties to the litigation that prohibits them from using or disclosing the information for any purpose other than the litigation *and* requires that the information either be returned to the covered entity or destroyed at the end of the litigation. *Id.* § 164.512(e)(1)(v).

122. 735 ILL. COMP. STAT. 5/8-802 (2005).

123. Neither side attempted to invoke any of the exceptions. *See* Nat'l Abortion Fed'n v. Ashcroft, No. 04C55, 2004 U.S. Dist. LEXIS 1701, at *12 (N.D. Ill. Feb. 5, 2004), *aff'd sub nom.* Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004).

124. *See, e.g.*, 410 ILL. COMP. STAT. 50/3(a) (2005) (granting patients a right to the confidentiality of their medical records, unless otherwise provided by law).

125. 210 ILL. COMP. STAT. 85/6.17(d) (2005).

126. *See* 45 C.F.R. § 160.202 (2005).

127. *Nat'l Abortion Fed'n*, 2004 U.S. Dist. LEXIS 1701, at *12.

128. *Id.* at *15.

controlled, the subpoena was quashed, and the records were not disclosed.[129]

On appeal, the Seventh Circuit affirmed the district court's quashing of the subpoena, but rejected its reasoning.[130] Unlike the district court, Judge Posner held that HIPAA did not constitute an Act of Congress for the purposes of Federal Rule of Evidence 501.[131] Although Judge Posner did not clarify what he thought "Act of Congress" meant in this context, he reasoned that the HIPAA rules for disclosure in judicial proceedings were merely procedural—simply a means of obtaining the authority to use medical records in litigation.[132] Whether the records would actually be admissible would depend on evidentiary privileges. Under Federal Rule of Evidence 501—which did not recognize a physician-patient or hospital-patent privilege—the federal common law was the controlling source of privileges.[133] The court stated that while Illinois could enforce its stringent evidentiary privilege in state court and in federal diversity cases in which state law controlled, state law provisions did not govern in federal question suits.[134]

Judge Posner then affirmed the quashing of the subpoena by fashioning a "relative hardship" balancing test under Federal Rule of Civil Procedure 45(c)(3)(A)(iv) and decided that the burden of compliance with the subpoena, together with the potential harm to the subjects, far exceeded the probative value or benefit of the material sought.[135] Thus, unlike the district court, for which the relative stringency of the federal and state standards was dispositive, the Seventh Circuit never even reached the question, because it decided that HIPAA was irrelevant to the case. Under Judge Posner's balancing approach, the substantive requirements of the Illinois provision were also largely irrelevant.[136]

129. *Id.* at *15–17.

130. *See* Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923, 925 (7th Cir. 2004) (stating, in contrast to the Illinois district court, "[W]e agree with the government that the HIPAA regulations do not impose state evidentiary privileges on suits to enforce federal law.").

131. *Id.* at 925–26.

132. *See id.* at 925.

133. *Id.* at 926.

134. *Id.* at 925. For the definition of a "federal question" case, see *infra* note 142.

135. *Nw. Mem'l Hosp.*, 362 F.3d at 928–33.

136. The court did state that the fact that the quashing of the subpoena was in accordance with Illinois law was a "final factor" in favor of affirming the district court's ruling. The court reasoned that because recognition of the Illinois provision could "'be accomplished at no substantial cost to federal substantive and procedural policy,'" the principles of comity demanded that the court do so. *Id.* at 932 (quoting Mem'l Hosp. v. Shadur, 664 F.2d 1058, 1061 (7th Cir. 1981)).

2. The New York Ruling

New York law expressly provides that unless the patient waives the privilege, a health care provider "shall not be allowed to disclose any information which he acquired in attending a patient in a professional capacity, and which was necessary to enable him to act in that capacity."[137] None of the statutory and common law exceptions to this law applied to the case.[138] Thus, like its Illinois counterpart, the New York law seemed to fit the definition of "more stringent" because it would not allow disclosure without patient consent in a situation where HIPAA would allow for such disclosure.

Nonetheless, like the Seventh Circuit, the trial court in the Southern District of New York also failed to reach the question of whether a state law is "more stringent" than HIPAA. In rejecting the idea that the New York law might be a factor in the disposition of the case, the trial court stated that HIPAA did not incorporate contrary state law.[139] It distinguished between a federal law that simply does not preempt a state law and therefore "merely allows [it] to continue to operate in its sphere of influence, unaffected by the federal statute," and a federal law that expressly incorporates a state law, thus giving the state law binding force that it might not otherwise have.[140] In the absence of HIPAA, New York state law would have had absolutely no force in the case at hand[141] because the case concerned a federal question being heard in federal court.[142] The issue for the court was whether HIPAA incorporated the state law, giving it a new and binding relevance in the dispute that it would not otherwise have had.[143]

137. N.Y. C.P.L.R. 4504(a) (Consol. 2003).

138. Nat'l Abortion Fed'n v. Ashcroft, No. 03 Civ. 8695 (RCC), 2004 U.S. Dist. LEXIS 4530, at *10–11 & n.5 (S.D.N.Y. Mar. 18, 2004), *aff'd sub nom.* Nat'l Abortion Fed'n v. Gonzales, No. 04-5201-CV, 2006 U.S. App. LEXIS 2386 (2d Cir. Jan. 31, 2006). These other exceptions include requiring providers to disclose information indicating that a patient under the age of sixteen had been the victim of a crime, *see* N.Y. C.P.L.R. 4504(b), and allowing disclosure for the purpose of investigating Medicaid fraud, *see* Camperlengo v. Blum, 436 N.E.2d 1299, 1301 (N.Y. 1982).

139. *Nat'l Abortion Fed'n*, 2004 U.S. Dist. LEXIS 4530, at *13–17.

140. *Id.* at *13.

141. *See id.* at *12–13.

142. A federal question case is one in which the judicial question arises under the U.S. Constitution or another source of federal law, such as a federal statute or treaty. *See* 28 U.S.C. § 1331 (2000). Federal question cases in federal court are the classic example of a domain in which state law, in the absence of incorporation, does not apply. Because the underlying dispute in the *National Abortion Federation v. Ashcroft* cases was a challenge to the constitutionality of the Partial-Birth Abortion Ban Act of 2003, they implicated a pure federal question. In addition, they were being heard in federal court.

143. *See Nat'l Abortion Fed'n*, 2004 U.S. Dist. LEXIS 4530, at *12–13.

The court distinguished laws containing "express" preemption language, which explicitly permits state standards to preempt federal law, from those containing the "negative" HIPAA language, which mandates federal preemption of state law *except* when the state law is more stringent.[144] Since HIPAA had no explicit "language of incorporation," the court deferred to HHS, which argued that HIPAA did not incorporate state law.[145] The court thus ruled that "the negative language in [HIPAA's preemption provision] does not equate to the positive power to create binding law in the federal domain—here, a case arising under federal law brought in federal court."[146] Thus, because the New York law would have had no impact in the absence of HIPAA and it had no effect after HIPAA, the case was instead governed by Federal Rule of Evidence 501.[147] Like the Seventh Circuit, but unlike the Illinois district court, the New York district court refused to "give any more effect to state law than it would have had in the absence of HIPAA."[148]

The further reasoning of the New York court, however, diverged sharply from the Seventh Circuit's analysis. The New York court agreed with the Illinois district court and disagreed with Judge Posner, stating that "Congress has spoken on the privacy of medical records through HIPAA," and that HIPAA therefore trumped the federal common law under Federal Rule of Evidence 501.[149] For the New York court, the dispositive factor was that the court had previously, in response to the original subpoena, issued a court order permitting disclosure, along with a protective order permitting the use of the information solely for the purposes of the litigation and requiring the destruction or return of the records within sixty days of its resolution.[150] The court held that the latter constituted a "qualified protective order," as defined by HIPAA.[151] Therefore, because the HIPAA regulations permitted the release of information once such a protective order was obtained, the subpoena was enforceable, and the records were disclosed.[152]

144. *Id.* at *13.

145. *Id.* at *14–17. The court reasoned that precedent requires courts to "defer to reasonable constructions of a statute, ambiguous or silent on an issue, made by the administrative agency responsible for administering it." *Id.* at *17.

146. *Id.* at *13.

147. *Id.* at *12–13.

148. *Id.* at *17.

149. *Id.* at *19–20.

150. *Id.* at *20–21.

151. For the definition of "qualified protective order," see *supra* note 121.

152. *Nat'l Abortion Fed'n*, 2004 U.S. Dist. LEXIS 4530, at *20–21.

It is difficult to reconcile the inconsistent rationales and rulings in these three opinions. Because they originated from the same underlying dispute, the subpoena at issue in the Illinois case was subject to the same court order and "qualified protective order" that the New York court found sufficient to comply with HIPAA. However, since the Illinois district court, alone in applying the "more stringent" test, decided that Illinois law controlled, the fact that the subpoena satisfied the HIPAA requirements for disclosure was irrelevant because the stricter Illinois law completely prohibited disclosure without patient consent. The courts also diverged in their treatment of the relationship between HIPAA and Federal Rule of Evidence 501, and in their approaches to the question of incorporation analyzed at length in the New York ruling. And while each ruling involved a state statute that appeared to meet the statutory definition of "more stringent," only the Illinois district court reached and applied the relative stringency test.

These related cases demonstrate that courts lack a standard analytical approach to analyzing preemption questions.[153] Some practitioners fear that as more litigation occurs, "a patchwork of varying decisions likely will emerge, and it remains to be seen the degree to which common themes will surface."[154] For example, "federal courts [may] be more inclined to give effect to the HIPAA Privacy Rule, a federal regulation, while state courts [may] lean toward giving effect to state requirements."[155] Judicial biases and preferences may also affect outcomes. For example, in disputes like the Ashcroft cases, which involved the highly politicized issue of partial-birth abortion, "'liberal' courts [might be] more inclined to rule that more stringent state law was applicable."[156]

To the extent that systematic differences emerge in the approaches taken by federal versus state courts, or different circuit courts, the lack of uniformity may lead to forum shopping and an inequitable application of the law. This is problematic because, when conflicts arise, "ultimately the final arbiter of whether a law is more stringent will be the courts."[157]

153. Although these cases probably could not have been properly consolidated and tried together, other sets of cases "involving a common question of law or fact" might qualify for consolidation. *See* FED. R. CIV. P. 42. This would help to address the problem of different courts applying different analytical frameworks to similar or related disputes, and thus help to reduce uncertainty. *See also, e.g.*, *Interplay Between HIPAA and State Law Uncertain*, *supra* note 12, at 4–6 (discussing, from a practitioner's point of view, the conflicting analytical approaches courts have taken).

154. *Interplay Between HIPAA and State Law Uncertain*, *supra* note 12, at 4–6.

155. *Id.*

156. *Id.*

157. *See* WHITE PAPER, *supra* note 66, at 7.

Courts will have the final responsibility not only for interpreting and applying the regulations, but also for shaping their meanings; it is critical that they do so in a uniform manner. Only then will their decisions provide the guidance that covered entities desperately need as they struggle to comply with the labyrinthine regulatory scheme.

## IV. COMPLETE PREEMPTION: IS IT THE ANSWER?

To many, the partial preemption framework is so unworkable that radical change seems to be the only viable solution. Critics of partial preemption argue that federal HIPAA regulations should constitute a single, comprehensive source of law that supersedes all state laws. They note that complete preemption would provide administrative ease and efficiency, clarity, practicality, predictability, and uniformity.[158] The battle lines of this debate are fairly well demarcated: Republicans and industry groups such as health plans, health care clearinghouses, and employers argue for complete preemption, while Democrats, patient advocates, state government representatives, and health care providers support partial preemption.[159] But in elevating uniformity and ease of administration above other considerations, the former group ignores issues such as the principles of federalism, the value of state innovation, and the need to preserve privacy protections that patients currently enjoy.

Respect for the principles of federalism demands that attention be paid to states' rights. HIPAA served to "effectively inject[] the federal government into an arena that had previously been primarily occupied by the states."[160] Complete preemption would allow the federal government to completely usurp the traditional state regulatory role. The partial

158. *See Privacy Standards Hearing*, *supra* note 12, at 11–12 (reporting that more than half of the forty stakeholder groups that commented on the proposed HHS Privacy Rule called for complete preemption, criticizing partial preemption as overly burdensome and excessively costly); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,579 (Dec. 28, 2000) (stating that "numerous" public comments rejected the partial preemption framework as burdensome, ineffective, or insufficient, and called instead for complete preemption of "patchwork" state laws); Guthrie, *supra* note 34, at 157 (stating that complete preemption "would give a sense of conformity to the existing 'patchwork' of state privacy laws"); Bishop, *supra* note 11, at 729 (asserting that the "need for uniformity, efficiency, and protection of patients' medical records serve[s] as evidence that the best solution to the present HIPAA confusion is one set of federal regulations that fully supplant state law"). *Cf.* Sharon J. Hussong, Note, *Medical Records and Your Privacy: Developing Federal Legislation to Protect Patient Privacy Rights*, 26 AM. J.L. & MED. 453, 469 (2000) (noting, "Insurance companies claim that federal preemption would ensure that they would not have to increase costs for consumers.").

159. *See Privacy Standards Hearing*, *supra* note 12, at 11; Scott, *supra* note 9, at 514–15; Hussong, *supra* note 158, at 467.

160. *See* Pritts, *supra* note 9, at 340.

preemption framework, on the other hand, attempts to balance the autonomy of the states against the need for uniform national standards on medical privacy.[161] Unlike complete preemption, partial preemption preserves the rights of states to legislate in this arena. In fact, states have reacted to HIPAA by either tweaking their existing laws or passing new, "more stringent" provisions that would survive preemption.[162]

In the context of patient privacy, the argument for protecting states' rights is not based solely on abstract historical, political, and policy arguments about the value of federalism. Complete federal preemption would also undermine the goal of increasing patient privacy protections. This Note assumes that privacy legislation and regulation should have the overarching purpose of optimizing the level of individual protection.[163] Complete preemption would have the opposite effect.

For example, as already discussed, many states have perceived a need for greater protection of those persons with medical conditions that have particular social or economic impact such as HIV/AIDS.[164] These states have accordingly adopted condition-specific laws that offer more protection than the federal standards. Furthermore, compared to the Privacy Rule, many state laws provide patients with greater protection against the unauthorized disclosure of their medical records.[165] This was certainly the case in Illinois and New York, where the legislatures had opted to safeguard the confidentiality of patient records to a greater degree than the HIPAA standards did.[166] Partial preemption respects a state's desire to offer such enhanced protection in an area it deems important, while ensuring a minimum federal level of protection. In contrast, complete preemption would eviscerate more protective state provisions, disregarding

161. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 60,047 (Nov. 3, 1999).

162. Ratner, *supra* note 28, at 543; Bishop, *supra* note 11, at 748.

163. A discussion of the optimum level of privacy protection is beyond the scope of this Note, which assumes for the purpose of argument that increasing the overall level of protection is desirable and that stronger protections are better than weaker ones. This point is somewhat controversial. For an argument that increasing the level of protection granted to individuals might not be socially beneficial, see Scott, *supra* note 9, at 491–505 (arguing that, because strict privacy protections have substantial social costs, it may be worth sacrificing some protection of individuals for the sake of the public benefits derived from lesser privacy protection, such as safeguarding the public health, facilitating medical research, assisting law enforcement efforts, and improving health care quality, access, and accountability). A less protective regime may be attractive for efficiency reasons. For example, the resources needed to ensure compliance might be better spent on the direct provision of health care.

164. *See supra* note 57 and accompanying text.

165. Hussong, *supra* note 158, at 468.

166. *See supra* Part III.C.

a state's determination of the value of additional protection and leaving its citizens with only the lower federal floor of protection.

Complete federal preemption also would invalidate state privacy protections that predate HIPAA. Patients should not be stripped of the more stringent rights that they have enjoyed by virtue of living in a state with more restrictive rules, especially when those protections concern sensitive social issues that federal regulations do not adequately address.[167] For example, one patient advocate predicted that federal preemption of California's HIV/AIDS confidentiality laws would precipitate a public health crisis by removing protections that encourage people to seek testing, counseling, and treatment.[168]

Complete preemption would not only eliminate preexisting state laws, but also would prevent states from passing new ones—presumably more stringent than the federal standards—in response to changing conditions. It would freeze the level of patient privacy at the point currently provided by HIPAA, instead of allowing states to innovate and offer enhanced protections. Compared to Congress, states may be more flexible, quicker to act, and generally more responsive to the needs of their individual citizens. States can specialize in innovative and "creative problem-solving" that may allow them "to counter new threats to patient privacy as they arise."[169] Therefore, while Congress would remain free to legislate under a complete preemption framework, preventing states from doing so would undermine the goal of enhancing patient privacy protections.

Much of the recent state legislative action has been in response to perceived gaps and weaknesses in the Privacy Rule.[170] For example, one of the major criticisms of the Privacy Rule is that it imposes few restrictions on the use and disclosure of health information for marketing purposes, allowing providers to use patient information for such activities without consent.[171] Both Florida and Texas responded by passing legislation requiring written consent for the use of protected information for marketing purposes.[172] Similarly, while the Privacy Rule authorizes civil and criminal sanctions, it has been criticized for not providing a federal private right of

167. *See Final HHS Regulation Hearing*, *supra* note 59; Bishop, *supra* note 11, at 742.

168. Geri Aston, *Battle Lines Drawn over Bills on Medical Records Privacy*, AM. MED. NEWS, May 10, 1999, at 1, 34 (quoting Chris Koyanagi, Policy Director of the Judge David L. Bazelon Center for Mental Health Law, Washington, D.C.).

169. Bishop, *supra* note 11, at 748.

170. Pritts, *supra* note 9, at 344–47.

171. *Id.* at 344.

172. *Id.* at 346–47.

action.[173] Texas responded to this concern with a statute that expressly grants individuals the right to bring causes of action or to seek other relief for violations of the state law.[174] Thus, states have asserted their legislative power to address perceived failings in the federal rule, thereby enhancing the level of privacy protection afforded to their citizens. Complete preemption would have left them powerless to do so.

By imposing a single national standard, complete preemption would ensure greater uniformity, but at the cost of reducing the overall level of privacy protection.[175] Many commentators argue that HIPAA, with its current partial preemption framework, will impose substantially more uniformity than existed before HIPAA. They note that a strong federal law will provide a substantial amount of predictability and uniformity simply by preempting similar or weaker state laws[176] and leaving a federal standard in their place. The federal floor will diminish the pre-HIPAA patchwork of regulations by harmonizing inconsistent state laws.[177] The overall effect will be that covered entities "will no longer have to worry as much about the fifty different state laws, because the weaker laws will fall out, and those more condition-specific or disease-specific laws that the states have passed . . . will continue to be in place."[178] Thus, commentators argue, over time, "substantial uniformity will be achieved."[179] The critical state provisions that are more stringent than HIPAA will remain in effect, ensuring that under partial preemption, greater uniformity does not require the sacrifice of potent individual provisions.

173. *See Final HHS Regulation Hearing*, *supra* note 59 (statement of Janlori Goldman, Director of the Health Privacy Project, Institute for Healthcare Research and Policy at Georgetown University) (arguing that the lack of a private right of action is "a serious impediment to accountability and a serious impediment to making this regulation real in people's lives").

174. Pritts, *supra* note 9, at 346–47.

175. It is possible for complete preemption to increase the overall level of privacy protection, but this would require federal legislation to contain more patient-protective provisions. As discussed *supra* note 163, the premise that greater protection is necessarily better is controversial. For various reasons, many favor lesser protection. Thus, enormous political obstacles would likely stand in the way of enacting extremely patient-protective national privacy standards.

176. Aston, *supra* note 168, at 34.

177. For example, a 1999 survey of state privacy laws found that while forty-four states provided patients with some right of access to their medical records, states varied widely in their approaches. PRITTS ET AL., *supra* note 49, executive summary. Thirty-three states gave patients access to hospital records, thirteen gave access to HMO records, and sixteen gave access to insurance records. *Id.* A strong federal law would help to address these inconsistencies by displacing the less stringent laws—that is, a single federal standard would replace the diverse state approaches.

178. *Final HHS Regulation Hearing*, *supra* note 59 (statement of Janlori Goldman, Director of the Health Privacy Project, Institute for Healthcare Research and Policy at Georgetown University).

179. *Id.*

Thus, partial preemption may not provide a greater degree of uniformity than complete preemption would, but it ensures significantly more uniformity than existed before HIPAA. More importantly, partial preemption offers the best balance of the relevant considerations. It respects states' rights and the principles of federalism, permits states to continue innovating in the arena of medical privacy, and allows them to respond legislatively to the perceived needs of their citizens. It also preserves certain pre-HIPAA regulations, such as condition-specific laws. In addition, states can offer enhanced privacy protection by regulating entities not covered by HIPAA and by enforcing privacy protections at the local level through state laws.[180]

While complete preemption advocates would readily sacrifice these benefits for the sake of uniformity and ease of administration, the partial preemption framework seems, at least for now, to be relatively safe. Complete preemption would require congressional action;[181] thus far, none has been forthcoming. Despite the widespread confusion imposed by the partial preemption framework, there have not yet been any concerted efforts to impose complete preemption. Nevertheless, if complete preemption advocates do become frustrated enough with the current scheme to begin actively lobbying for such a change,[182] they will seek to leverage their clout with a Republican-controlled Congress, already favorably disposed toward complete preemption. Furthermore, as the health care industry evolves, calls for uniformity may increase, necessitating congressional action.[183] Even President Bill Clinton and former HHS Secretary Donna Shalala, who presided over the enactment of the HIPAA rules, did not consider HHS rulemaking to be a "satisfactory long-term substitute for comprehensive legislation that could, and preferably would, be enacted by Congress in the future."[184]

The threat of complete preemption, while not imminent, looms on the long-term horizon, especially if the Republicans maintain control of Congress. For the time being, however, the partial preemption framework remains in place. While it imposes greater administrative burdens than would exist under complete preemption, there are ways in which partial preemption could be streamlined. A system could be implemented that

180. Pritts, *supra* note 9, at 348.

181. WHITE PAPER, *supra* note 66, at 18.

182. *See id.*

183. *Cf.* Scott, *supra* note 9, at 510 (suggesting that Congress enact comprehensive legislation in the area).

184. *Id.*

would reduce the costs of compliance while providing greater guidance and uniformity for covered entities and judges.

## V. IMPROVING THE PARTIAL PREEMPTION SYSTEM

The current partial preemption framework all but "ensures that clarity and simplicity are overcome by complexity and confusion."[185] There is, however, room for significant improvement in the system. Rather than imposing a controlling set of national standards, as complete preemption advocates suggest, the goal should be to create a uniform, streamlined, analytical framework for deciding preemption issues. Such a framework, which would require the cooperative efforts of Congress, HHS, and the individual states, would decrease the administrative burdens, confusion, and uncertainty in the system.

### A. CONGRESS SHOULD CLARIFY ITS INTENT WITH REGARD TO INCORPORATION

As it stands, partial preemption creates a "knotty tangle for courts to parse in years to come."[186] Congress can help alleviate some of the challenges that courts face by clarifying whether it intends for state law to be incorporated into federal law through HIPAA. Congress should clarify whether HIPAA absorbs "more stringent" state laws, thus giving them force where they would not otherwise operate—such as in pure federal question cases[187]—or whether HIPAA's reverse preemption provision merely allows state laws to continue operating in their own "sphere[s] of influence,"[188] retaining only the force they would have had without HIPAA.

That courts disagree on this question is clear,[189] but it is critical that a uniform approach be adopted because the issue may be dispositive in litigation—as was seen in the Partial-Birth Abortion Ban Act cases in New

185. Gallagher, *supra* note 48, at 8.

186. *HIPAA Privacy One Year Out*, *supra* note 21, at 2.

187. *See supra* note 142.

188. Nat'l Abortion Fed'n v. Ashcroft, No. 03 Civ. 8695 (RCC), 2004 U.S. Dist. LEXIS 4530, at *13 (S.D.N.Y. Mar. 18, 2004), *aff'd sub nom.* Nat'l Abortion Fed'n v. Gonzales, No. 04-5201-CV, 2006 U.S. App. LEXIS 2386 (2d Cir. Jan. 31, 2006).

189. *Compare Nat'l Abortion Fed'n*, 2004 U.S. Dist. LEXIS 4530, at *14–17 (holding that state privilege law was inapplicable to a federal question case being heard in federal court), *with* Nat'l Abortion Fed'n v. Ashcroft, No. 04C55, 2004 U.S. Dist. LEXIS 1701, at *16–17 (N.D. Ill. Feb. 5, 2004), *aff'd sub nom.* Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004) (holding that state law controlled, thus implicitly deciding that state law applied in the dispute, even though it was a federal question case in federal court).

York and Illinois.[190] The New York district court noted that in previous legislation Congress had explicitly incorporated state standards into federal law,[191] but that HIPAA did not contain such explicit "language of incorporation."[192] Thus, Congress should clarify its intent with regard to the incorporation question by amending the language of HIPAA's preemption provision.

Alternatively, Congress could rely on HHS pronouncements to answer the incorporation question. HHS has stated:

> [W]e do not think that section 264(c)(2) would work to apply State law provisions to federal programs or activities with respect to which the State law provisions do not presently apply. Rather, the effect of section 264(c)(2) is to *give preemptive effect to State laws that would otherwise be in effect* . . . . Thus, we do not believe that it is the intent of section 264(c)(2) to give an effect to State law that it would not otherwise have in the absence of section 264(c)(2).[193]

Congress could simply announce its intention either to reject or defer to HHS's interpretation. This solution may be more efficient than amending the HIPAA language, and presumably, it would provide the same level of guidance for courts confronted with the incorporation issue.[194]

### B. HHS AND STATES SHOULD WORK TOGETHER TO CREATE STATE-BY-STATE PREEMPTION ANALYSES

Because much of the current preemption analysis is indeterminate, "[d]ifferent organizations, agencies and associations within a state could analyze their state's preemption situation and end up with different opinions."[195] With so much room for disagreement, both compliance and

190. *See supra* Part III.C.

191. *Nat'l Abortion Fed'n*, 2004 U.S. Dist. LEXIS 4530, at *14. For example, the court noted that the Assimilative Crimes Act of 1948 expressly rendered violations of state and local law committed on federal territory federal crimes, and that the Outer Continental Shelf Lands Act of 1978 similarly declared that state civil and criminal laws are to be given federal effect in waters off the nation's coast, so long as they do not conflict with federal law. *Id.* (citing 18 U.S.C. § 13 (2000) and 43 U.S.C. § 1333(a)(2)(A) (2000)).

192. *Id.* at *15.

193. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 60,000 (Nov. 3, 1999) (emphasis added) (citing Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, § 264(c)(2), 110 Stat. 1936, 2021 (codified as amended in 42 U.S.C. § 1320d-2 (2000)).

194. For example, the court in the Southern District of New York deferred to HHS's interpretation that HIPAA does not incorporate state law. *Nat'l Abortion Fed'n*, 2004 U.S. Dist. LEXIS 4530, at *16–17.

195. *See* WHITE PAPER, *supra* note 66, at 17.

enforcement efforts would be greatly facilitated by the existence of authoritative analyses. Therefore, state officials, stakeholders, and HHS should work together to create one analysis per state that would be certified as official and made available for public use.[196] Certification would essentially provide these analyses with the force of law.[197] States would agree not to take action against any covered entity that complied with the official analysis; the analyses would likewise be binding on courts and on OCR.[198] Therefore, covered entities that relied in good faith on the certified results would be immunized from potential liability for noncompliance with the Privacy Rule.[199]

The certification process would require a great deal of collaboration—and ultimately agreement—among its participants.[200] State officials or some representative state body would begin by compiling all relevant state laws, including statutes and regulations, common law, and local laws.[201] This burden should fall on state officials because they, rather than HHS, would likely have a greater understanding of the current patchwork of privacy protections in their own jurisdictions.[202] The goal would be to

196. Guthrie, *supra* note 34, at 153–54 (proposing a collaborative effort between covered entities, state governments, and HHS to creating binding preemption analyses on a regular schedule). Several states have already begun taking a collaborative approach to the problem of preemption analysis. *Id*. at 153–54 & n.45. *See also* WHITE PAPER, *supra* note 66, at 14 (discussing a similar cooperative venture currently underway in Illinois).

197. *See* Guthrie, *supra* note 34, at 154 (suggesting that "HHS could review each interpretation and certify the analyses that are validly completed"). The American Academy of Family Physicians submitted a similar certification suggestion to the HHS Regulatory Advisory Committee in February, 2000. *Id.* at 154 n.46.

198. *Cf. id.* at 154 (proposing 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"). Requiring that OCR be legally bound by the results of the certification analyses would necessitate amendments to the Privacy Rule and possibly to the underlying HIPAA legislation. A certification process was proposed to HHS, but it was deleted from the final rule. *See id.* at 154 n.47.

199. *See id.* at 154.

200. *See id.* at 153–54. The process would essentially culminate in federal and state agreement on results that would then assume the force of law. While this may require specific authorizing legislation by Congress or may raise other administrative law issues, these topics are beyond the scope of this Note.

201. *See id.* at 153; WHITE PAPER, *supra* note 66, at 14 (discussing a similar effort in Illinois). Each state would be responsible for designating the state officials or body that would complete this work. For example, California's Health and Safety Code requires the California Office of HIPAA Implementation ("CalOHI") to assume statewide leadership, coordination, direction, and oversight for the implementation of HIPAA provisions. *See* CAL. HEALTH & SAFETY CODE §§ 130302–130303 (West Supp. 2005). Therefore, CalOHI would presumably take the lead in compiling all California state law provisions for the certification process.

202. As a practical matter, the task of fully surveying the states' privacy laws will leave these state bodies with a much greater understanding of the depth and breadth of their privacy protections,

ensure both breadth and depth of coverage. Thus, states ideally would collaborate in this task with state medical associations, industry organizations, local officials, health care providers and insurers, professional associations, and other groups that may have expertise in the relevant areas of law.[203] In most cases, the states would not be starting from scratch because they could rely, in part, on compilations of state laws from preemption analyses that are already available.[204] While existing compilations would not be exhaustive for the purposes of a provision-by-provision comparison,[205] their use would allow the states to conserve resources by building on work that already has been done and simply filling in the gaps.

Once the state law provisions were compiled, the real collaboration between HHS and the states would begin.[206] HHS would be primarily responsible for conducting the provision-by-provision comparison of state laws and the Privacy Rule, and for determining which state provisions are more stringent than their HIPAA counterparts. The certification of such determinations would be binding on states, which would in turn lose the ability to enforce state law provisions that the certified analyses held to be preempted. States, therefore, would have a strong incentive to participate in the process. Once HHS and the states made their final determinations, the analyses would be certified and made available to the public.[207]

providing them with an ideal starting point, should they wish to consider further legislation in this arena.

203. *See* Guthrie, *supra* note 34, at 153. Strictly speaking, stakeholder participation in certification would not be required; organizations may refuse to become involved. Because, however, many of these groups represent covered entities and would be directly affected by the results of the certification analysis, they would presumably welcome the opportunity to be involved.

204. For example, CalOHI has completed preemption analyses involving the major California privacy statutes, such as the Confidentiality of Medical Information Act, CAL. CIV. CODE § 56 (West 1982), and the California Public Records Act, CAL. GOV'T CODE § 6250 (West 1995). *See* California Office of HIPAA Implementation—Legal Issues, *supra* note 72.

205. Some of these analyses do not cover all provisions of "state law" as defined by the Privacy Rule, and therefore would not constitute an exhaustive list for the purposes of the certification process. *See, e.g.*, 50 State HIPAA Privacy Study, *supra* note 77; California Office of HIPAA Implementation—Legal Issues, *supra* note 72.

206. *See* Guthrie, *supra* note 34, at 154.

207. As the certification process would be extremely resource-intensive, it would be preferable for HHS to be able to recoup some of its costs by charging covered entities for access to the results. But because the analyses, once certified, would have the force of law, the possibility of forcing users to pay in order to determine what the law is raises serious constitutional concerns. Such a discussion is beyond the scope of this Note. This Note simply raises the possibility that HHS could impose a sliding scale through which the price that a covered entity paid for access would depend on factors such as the entity's size. The fee schedule would balance the competing concerns of the covered entity's ability to pay with the needs of HHS and the states to recover their costs.

Because both state laws and the federal standards will continually change, the process will require a mechanism to ensure that analyses are current. Annual updates balance the need for maintaining current analyses with the costs of continually monitoring developments in the law. States would be responsible for notifying HHS of new state law provisions or changes to existing laws. Because any changes to the actual Privacy Rule would originate with HHS, the agency itself would be responsible for monitoring changes in the federal law. Once a year, HHS would perform new provision-by-provision comparisons, as necessary, and incorporate updates into the analyses. As with the initial analyses, the updates would also be subject to state agreement before being certified for public use.

The final aspect of the system would be a mechanism by which, if a covered entity were unable to find sufficient guidance on a specific situation in the official analysis, then the entity could obtain an authoritative response on which it could rely.[208] These authoritative responses would be issued by the same agency responsible for the certified analyses, and they would have the same force of law. Thus, covered entities would be immunized from potential liability by compliance with an official HHS determination.

The certification process would provide substantial uniformity by creating a single authoritative analysis in each state. The implemented system would provide covered entities with one credible and complete source for information. This would significantly reduce search costs and eliminate the need for entities to either undertake their own burdensome analyses or to seek outside assistance. It would also greatly reduce the potential liability of covered entities, which currently assume the risk of relying on incorrect preemption analyses.

The annual update mechanism would address the potential compliance challenges that a constantly changing regulatory landscape raises. State and federal law changes would be reported once a year, and covered entities would not be responsible for compliance with those laws until they have been incorporated into the annual update. Users would have to comply only with the most recently issued analysis. Thus, if a user relies on the most recent certified analysis, the user would be immunized from liability for violating regulations that postdate that analysis. The user would only be

208. *Cf.* Guthrie, *supra* note 34, at 155–56 (discussing a similar advisory opinion process that was initially included in the proposed regulation, but removed from the final rule). For further discussion of this abandoned opinion process, see *infra* notes 210–12 and accompanying text.

liable under newly promulgated regulations or newly enacted legislation when that authority has been incorporated into an official analysis.

There is no denying that the costs of implementing a certification process would be high, particularly at the beginning. Nevertheless, while the system would require substantial upfront expenditures, primarily for performing the initial analyses, the costs would diminish after the initial set of analyses were certified. Subsequently, the only significant administrative expenses would be completing the annual updates and issuing authoritative responses to covered entities' inquiries. Furthermore, many stakeholders argue that HHS should bear the costs of compliance with the preemption provision.[209] This certification system would shift responsibility from covered entities—which now bear 100% of both the costs of compliance and the risks of noncompliance—to the states and HHS. This shift would be a vast improvement over the current system, which is relatively insensitive to whether covered entities can afford to comply with the preemption requirements.

In addition, under the current system, every covered entity must expend significant resources to conduct its own preemption analysis. By contrast, the certification system would require only one analysis per state or jurisdiction, and would therefore substantially reduce the wasteful duplication of efforts and resources that results when multiple entities are forced to perform essentially redundant analyses. Presumably, the system would also diminish the number of complaints that OCR receives, thereby reducing the costs of investigation and enforcement. Likewise, the proposed system would diminish the need for the educational and technical assistance that OCR currently provides to covered entities. Finally, this process would help to decrease disputes over the interpretation of the preemption provision. It would thus conserve judicial resources by reducing—and hopefully by eliminating—the need for litigation on preemption issues. Therefore, because resources used to implement the certification process would be conserved elsewhere, the system may not be as expensive as it initially appears.

209. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,583 (Dec. 28, 2000) (noting that many of those commenting on the proposed rule argued that HHS should bear the cost of preemption analysis, disagreeing with the premise that it was more efficient for the private market to do so). *See Final HHS Regulation Hearing*, *supra* note 59 (statement of Jane Greenman, Deputy General Counsel, Honeywell International, Inc., representing the American Benefits Counsel) ("[I]t's not realistic or desirable to place the burden on each regulated entity to try and sort out whether federal or state standards apply . . . . Imagine, if it's too burdensome for HHS, how burdensome it would be for individual employers.").

As an initial matter, congressional action would almost certainly be required to ensure HHS participation in the certification process. In the proposed rule, HHS had planned to accept requests for advice from states, issuing advisory opinions which would represent the agency's determinations on the issues raised.[210] HHS considered that its mandate gave it clear authority to issue such advisory opinions.[211] Despite widespread support, however, HHS opted to eliminate the advisory opinion process because it feared that entities would treat the results as dispositive, even though the opinions would not have been binding on courts. Additionally, HHS was concerned that the burden of producing such opinions would have been a "non-optimal allocation" of HHS resources.[212] Since then, HHS has taken the strong stance that it is the responsibility of covered entities to perform their own preemption analyses. It has stated:

> [HHS does] not agree that the task of evaluating the requirements [of the Privacy Rule] in light of existing state law is unduly burdensome or unreasonable. Rather, it is common for new federal requirements to necessitate an examination by the regulated entities of the interaction between existing state law and the federal requirements.[213]

The authority HHS would need to participate fully in the certification process far exceeds the authority necessary to issue a nonbinding advisory opinion. Furthermore, given HHS's belief that covered entities are responsible for performing their own preemption analyses, congressional action would likely be required to contravene HHS's stated rationale for abandoning the advisory opinion process. Because advisory opinions were not binding, they could not guarantee outcomes for users. In contrast, covered entities, enforcement officials, and judges could rely on analyses certified jointly by HHS and individual states. As an initial step, Congress

210. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,998 (Nov. 3, 1999); Guthrie, *supra* note 34, at 155.

211. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,587. In response to public comments that questioned whether HHS had standing to issue binding advisory opinions, the agency responded as follows:

> [W]e disagree that the Secretary lacks legal authority to opine on whether or not state privacy laws are preempted. The Secretary is charged by law with determining compliance, and where state law and the federal requirements conflict, a determination of which law controls will have to be made in order to determine whether the federal standard, requirement, or implementation specification at issue has been violated. Thus, the Secretary cannot carry out her enforcement functions without making such determinations.

*Id.*

212. *Id.* at 82,580; Guthrie, *supra* note 34, at 155.

213. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,583. *See also Final HHS Regulation Hearing*, *supra* note 59 (statement of Leslie G. Aronovitz, Director, Health Care Program Administration and Integrity Issues) (observing that "[HHS does] feel that it's the covered entities' responsibility to make those determinations on their own").

would have to broaden HHS's mandate to authorize the issuance of authoritative and binding determinations. Furthermore, Congress would have to force HHS to assume responsibility in this arena. In all likelihood, additional resources would have to be allocated to HHS to ensure that it was fully equipped to fulfill its new role.[214]

## VI. CONCLUSION

The problems raised by the current partial preemption framework cannot be denied. The benefits of HIPAA come at a substantial cost to covered entities, which "must adhere to the significant, time-consuming, often convoluted, and administratively and precedentially undeveloped compliance requirements."[215] The preemption provision forces covered entities to perform a highly technical and dangerously indeterminate analysis without adequate guidance or support. At the same time, courts, which have the final say in disputes, lack guidance on crucial issues such as operational definitions and the question of whether HIPAA incorporates state laws.

The unfortunate state of the regulatory framework has led to calls for complete federal preemption. But the costs of complete preemption would far exceed its benefits, resulting in a significant decrease in the overall level of privacy protection that citizens enjoy. The optimal balance of the relevant considerations—states' rights, uniformity and ease of administration, the need to preserve existing patients' rights, and the value of flexibility and innovation—can be struck within the existing partial preemption scheme. This accomplishment will require the collaborative efforts of Congress, HHS, states, and stakeholders in clarifying problematic issues and implementing a uniform framework for analysis through the certification process.

Instead of the single comprehensive federal standard that complete preemption advocates suggest, certification would result in fifty sets of standards, one for each state, allowing for the complementary coexistence of the federal floor standards and more protective state laws.

Conceptually, the certification process should not be thought of as producing a right answer to preemption questions. In many cases, due to the indefiniteness of the analysis, there will be no such thing. Rather,

214. HHS might have to supplement its own personnel with outside legal counsel, hired on a time-limited basis, to perform the bulk of the analysis.

215. United States *ex rel.* Pogue v. Diabetes Treatment Ctrs., No. 99-3298, 2004 U.S. Dist. LEXIS 21830, at *15 (D.D.C. May 17, 2004).

certification should be viewed as a process by which agreement on thorny preemption issues can be reached. Reaching such a consensus is the key to easing the administrative burdens and interpretive challenges that the partial preemption framework currently presents. Only then can HIPAA realize its twin goals of allowing the United States to maintain its longstanding tradition of recognizing and respecting patient privacy while also increasing the efficiency and effectiveness of the health care system.