BNA's

HEALTH CARE POLICY

BNA Employee-Owned Since 1947

VOL. 15, NO. 11 REPORT MARCH 19, 2007

Health Information

Does HIPAA Preemption Pose a Legal Barrier To Health Information Transparency and Interoperability?

BY SARA ROSENBAUM, JD; PHYLLIS C. BORZI, JD, MA; TAYLOR BURKE, JD, LLM; AND SONIA W. NATH, JD, MPH.

Executive Summary

This paper summarizes the results of a review of nearly 500 judicial opinions decided as of fall 2006, involving access to protected health information (PHI) and privacy of medical information under the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). This review was undertaken to determine whether HIPAA, which permits application of state privacy laws that are more stringent than the federal privacy standard, acts as a legal barrier to the creation of interoperable health information systems that permit transparency of health information. The availability of transparent and complete information regarding health system performance has been recognized as essential to improving the quality of care and reducing health care disparities.

This exhaustive review of existing HIPAA court decisions provides no evidence that allowing more stringent state laws to be enforced impedes providers' access to essential patient information. Nor does it create obstacles to the use of such information to improve quality, or to the aggregation and de-identification of such information for use in transparent reporting.

Out of 113 HIPAA preemption cases that squarely focus on an alleged conflict between the HIPAA privacy rule and state law, only 13 cases involve situations where the court views state laws as more stringent than HIPAA, and none of the decided cases involve the denial of access to providers who seek personal health information for the purposes of treatment, quality improvement, or the production of transparent information.

Indeed, HIPAA preemption litigation appears to focus on situations involving the disclosure of PHI as part of the legal process, rather than the use of this information to improve quality, reduce disparities, or create transparency. The most common type of case is one in which a health care provider is seeking to use HIPAA to shield

Sara Rosenbaum is the Harold and Jane Hirsh Professor and Chair, Department of Health Policy, the George Washington University School of Public Health and Health Services. Phyllis C. Borzi is a research professor in the Department of Health Policy, GWU School of Public Health and Health Services. Taylor Burke is an assistant research professor in the Department of Health Policy, GWU School of Public Health and Health Services. Sonia W. Nath is a recent graduate of the dual degree program in law and public health at GWU and is currently a judicial clerk. *This analysis was funded under a grant from the Robert Wood Johnson Foundation.*

PHI from disclosure or to obtain PHI to defend himself or herself in malpractice or tort liability litigation. There is no evidence that more stringent state privacy laws are precluding health care providers either from securing essential information at the point of treatment or from participating in health information transparency programs. Even in the few cases where state law has been found to be more stringent than the federal HIPAA privacy standard, courts uniformly underscore the power of providers to control data disclosure within the existing HIPAA framework without violating state law.

If anything, HIPAA—far from being undermined by the continued vitality of more stringent state laws—permits covered entities to substitute their own uniform policies for variable state disclosure laws. If covered entities desire to disclose the requested PHI, they generally can do so, either by adopting a disclosure policy that permits disclosure, by observing a state reporting requirement, or by exercising an exception to a state privilege law. Based on the cases under HIPAA to date, covered entities that do not want to disclose information stand an excellent chance of persuading a court that HIPAA classifies most disclosures as permitted and therefore, the decision to disclose is up to the entity. Whether covered entities understand or acknowledge their power to determine health information transparency and establish such norms is doubtful at this point, given the extensive litigation seeking clarification of duties and rights of covered entities under HIPAA.

Ultimately, states may desire to achieve greater uniformity where personal health information privacy standards are concerned. But the HIPAA preemption cases decided to date suggest that a federal effort to legislatively preempt state privacy standards would have limited relevance to the development of interoperable information systems or systems in which health information transparency is integral to quality improvement. Moreover, such an effort to preempt all state laws relating to privacy of individually identifiable medical information could mire the federal government deeply into questions of how the states' legal processes work and interfere with long-established state civil and criminal procedural rules regarding the disclosure of data in relation to malpractice and other liability claims.

Introduction

This analysis, part of the Robert Wood Johnson Foundation's ''Legal Barriers to Health Information'' project, examines the preemption provisions of HIPAA. Specifically, this analysis evaluates the extent to which HIPAA preemption poses a legal barrier to secure and interoperable[1] health information systems that can support quality improvement while also advancing the broad policy goal of public reporting of aggregated, de-identified data measuring progress in improving health care quality and reducing health care disparities.

The evidence reviewed in this analysis consists of nearly 500 judicial decisions decided as of November 2006 involving the HIPAA Privacy Rule. Of these cases, 113 involved interpretation of the HIPAA Privacy Rule as it relates to state laws governing personal health information.

Following a discussion of the background underlying this issue and the research methodology used to conduct our review, we examine cases that have focused on the issue of ''HIPAA preemption''—that is the provisions in HIPAA that address the relationship between the minimum federal standards governing the use and disclosure of certain individually identifiable health information (''protected health information'' or ''PHI'') and state laws.

HIPAA creates federal legal preemption of state laws that are ''contrary to'' HIPAA's privacy ''floor,'' while simultaneously saving from preemption state laws that establish ''more stringent'' privacy rights for individuals. However, misunderstandings about the breadth, scope, and content of HIPAA's basic rules, and the flexibility that covered entities have to design their own privacy policies appear to contribute to the perception that HIPAA and its preemption provisions may impede the development of interoperable and transparent health care information systems.

Finally, we conclude this analysis with a discussion of the implications of our findings for health information system transparency and interoperability.

Background

An Overview of HIPAA and its Preemption Provisions

Enacted in 1996, HIPAA was a far-reaching law with multiple aims, including improving health insurance portability, reducing health care fraud, and promoting the quality and efficiency of health care through administrative simplification and computerization of health care information.[2] Recognizing the compelling need to protect the privacy and security of personal health information in an era of electronic information transfer, Congress instructed the secretary of health and human services to develop regulatory standards. Following a lengthy public comment period, the secretary issued the final Privacy Rule,[3] which became final after a two-year

[1] As defined in a 2006 Executive Order issued by President Bush, the term ''interoperability'' means ''. . .the ability to communicate and exchange data accurately, effectively, securely, and consistently with different information technology systems, software applications, and networks in various settings, and exchange data such that clinical or operational purpose and meaning of data are preserved and unaltered.'' *Executive Order: Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs*, (Aug. 22, 2006), available at http://www.whitehouse.gov/news/releases/2006/08/20060822-2.html (Accessed Nov. 8, 2006).

[2] *See generally* Deborah F. Buckman, *Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder*, 194 A.L.R. Fed. 133 (2004).

[3] DHHS issued a proposed Privacy Rule for public comment on Nov. 3, 1999, and, after receiving and responding to more than 52,000 comments, issued a final Privacy Rule on Dec. 28, 2000 (65 Fed. Reg. 82462). After the new Bush administration took office, in March, 2002, DHHS proposed and released for public comment modifications to the final Privacy Rule. After reviewing the additional 11,000 comments, modifications were published in final form on Aug. 14, 2002 (67 Fed. Reg. 53182). An unofficial version of the HIPAA Administrative Simplification Regulation Text, 45 CFR Parts 160, 162, and 164, as amended through Feb. 16, 2006 (which includes the current version of both the Privacy and Security Rules) is available at http://dhhs.gov/ocr/hipaa/finalreg.html (Accessed Nov. 22, 2006).

   ISSN 1068-1213

transitional compliance period.[4] The Rule is primarily enforced by the Office for Civil Rights (OCR) within the Department of Health and Human Services (DHHS). Having overcome a series of legal challenges, the Privacy Rule today provides a basic national legal framework for patient health information privacy.[5]

Under the HIPAA framework, protected health information (PHI) is specifically defined and generally protected.[6] At the same time, however, PHI can be disclosed and transmitted through secure and interoperable electronic systems for a number of federally defined purposes, including treatment, payment, and health care operations, without written patient authorization.[7] Aggregated and de-identified health information also can be used in a variety of ways that advance public understanding of the quality of health care and the process of quality improvement.[8] In addition, the Privacy Rule specifies a number of ''public health and benefit activities'' that permit access to PHI by public health and public safety agencies, without written patient authorization and in clearly defined circumstances.[9] Sanctions can be imposed by the federal government for Privacy Rule violations,[10] but the law creates no private right of action for individuals to enforce federal protections or redress potential privacy violations.[11]

As with most laws grafted onto a complex and preexisting legal field, the HIPAA Privacy Rule functions as part of a broad body of law governing information privacy.[12] Indeed, health information privacy is one of the premier examples of the nation's intricate federal legal framework, blending together centuries-old judicial common law traditions with federal and state constitutional provisions and statutory law.[13] The HIPAA Privacy Rule is simply the latest and best-known arrival on the privacy law scene.

The sheer breadth and scope of health information law obviously can create legal uncertainty, a phenomenon that the health care system has lived with for decades. To begin to reduce some of this uncertainty and to foster greater uniformity, HIPAA essentially establishes a roadmap toward reconciling the legal diversity in the health information arena. This roadmap operates as follows: HIPAA generally preempts state laws that are ''contrary to'' its standards. At the same time, the law also specifies that HIPAA privacy standards do:

> *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 the regulation.[14] [emphasis added].

This legislative structure thus establishes a standard for determining when federal HIPAA standards are preemptive (i.e., when its standards take precedence over state law) and when they are not. Unlike the better-known and broader preemption provisions found in the Employee Retirement Income Security Act (ERISA), HIPAA does not simply sweep away all state laws that may somehow ''relate to'' the subject matter addressed by HIPAA.[15] Instead, HIPAA preempts only those state laws that are ''contrary to'' federal health information privacy standards, while preserving more protective state laws that may exist. Put another way, HIPAA establishes *a federal floor, but not a federal ceiling*, on personal health information privacy law. This approach to preemption has been upheld as a valid exercise of Congress's commerce clause powers and as not unconstitutionally vague.[16]

Revisiting HIPAA Preemption as Part of Health Information Technology Adoption Initiatives

Over the past decade, as interest has intensified in the creation of interoperable health information systems that can improve the quality of information and create greater information transparency, both public and private policymakers increasingly have focused on the actual and perceived legal barriers to achieving such a goal. Among the numerous actual and perceived legal barriers attracting policymakers' attention[17] have been possible barriers associated with the diffusion and uses of health information technology, including the adoption of the technology and its various uses.

In some cases, careful examination of the law has shown evidence of a possible, actual legal barrier, and steps have been taken to remove the barrier. A good example of this phenomenon is Congress's decision in 2003 (followed by HHS implementation two years later) of special ''safe harbors'' to protect the sharing of health information technology under certain circumstances.[18]

---

[4] ''Covered entities'' were required to comply by April 14, 2003. Small health plans were given an additional year to comply (April 14, 2004).

[5] *See Association of American Physicians and Surgeons, Inc. v. U.S. Dep't of Health and Human Services*, 224 F. Supp.2d 1115, 194 A.L.R. Fed. 711 (S.D. Tex. 2002), *aff'd without opinion*, 67 Fed. Appx. 253 (5th Cir. 2003).

[6] 45 CFR § 160.103.

[7] 45 CFR § 164.502(a)(1)(ii) and 45 CFR § 164.506.

[8] 45 CFR § 164.512(b)

[9] 45 CFR § 164.512 (b)

[10] 42 U.S.C. § 1320d-5 and 6.

[11] Although numerous federal district courts have rejected the proposition that HIPAA created a private right of action allowing individual suits to enforce the Privacy Rule, the first appellate decision affirming that principle recently was handed down by the U.S. Court of Appeals for the Fifth Circuit. *See Acara v. Banks*, 470 F.3d 569 (5th Cir. 2006).

[12] D. Solove, M. Rotenberg and P. Schwartz, *Information Privacy Law* (Aspen Pub. 2006).

[13] J. Hodge and K. Gostin, Challenging Themes in American Health Information Privacy, and the Public's Health: Historical and Modern Assessments; 32 J.L. Med. And Ethics 670 (Winter, 2004) ; A.C. Breckenridge, *The Right to Privacy* (Lincoln: University of Nebraska Press, 1970); R.R. Faden, T.L. Beauchamp, in collaboration with N.M.P. King, A History and Theory of Informed Consent (New York: Oxford University Press, 1986).

[14] In HIPAA, Congress added a new Section 1178(a) to Part C of Title XI of the Social Security Act that addresses preemption by describing this relationship between federal and state law. However, the most critical language addressing preemption in the privacy context is the language cited above in Section 264(c)(2) of HIPAA itself and incorporated by reference in new Section 1178(a)(2)(B) of the Social Security Act.

[15] ERISA § 514(a).

[16] *See South Carolina Medical Ass'n v. Thompson*, 327 F.3d 346 (4th Cir. 2003), cert. denied, 124 S. Ct. 464 (U.S. 2003).

[17] *See* Sara Rosenbaum et al., ''Charting the Legal Environment of Health Information,'' The Robert Wood Johnson Foundation, 2005, available at http://www.healthinfolaw.org (Accessed Jan. 7, 2007).

[18] For example, this legal problem was addressed (at least in part) by recently finalized Stark and anti-kickback safe har-

In other cases, research may show that legal barriers are more perceived than real; in these situations, clarification regarding how law should be applied to new situations may help reduce perceived legal barriers to the full and transparent use of health information. For example, a recent analysis found no actual federal legal barriers to the collection, analysis, and disclosure of racial and ethnic data in health care quality improvement, and recommended the development of clear federal guidance regarding the permissible uses and disclosures of race and ethnicity data as part of broad quality improvement efforts.[19]

In the area of interoperability and the full disclosure of aggregated and de-identified performance data, law once again has emerged as a perceived barrier. The basis for this concern is that more stringent state privacy might somehow prohibit the sharing of health information permitted by HIPAA or the use of such information to develop appropriate public sources of information about system performance.

This concern has led to recent federal legislative proposals that would begin to move U.S. health information law toward a more uniform and standardized vision of privacy. The legislation would accomplish this goal by developing and implementing federal standards to establish *both a legal floor and ceiling* on health information privacy. This movement toward uniformity of health information privacy law can be seen in the two leading measures considered but not enacted during the 109th Congress: the ''Wired for Health Care Quality Act,'' (S. 1418)[20] which passed the Senate in November 2005; and the ''Health IT Promotion Act,'' (H.R. 4157),[21] which passed the House in 2006. Both pieces of legislation reflect a concern that the goals of uniform interoperability and transparency would somehow be incompatible with stricter state privacy laws.[22]

Thus, the Senate measure, in reaffirming the current HIPAA preemption statute,[23] also would have required recommendations regarding uniform national policies for the ''protection of health information through privacy and security practices.''[24] The House bill similarly reaffirmed the current HIPAA privacy standard while also providing for a study of state privacy laws.[25] The House bill also required the HHS secretary to propose, and Congress to consider, legislation ''providing for greater commonality'' among federal and state law[26] in order:

> to ensure the availability of health information necessary to make medical decisions at the location in which the medical care involved is provided. . . .

In this regard, the House measure reflects legislative concern that state health information privacy law may be acting as a barrier to the use and disclosure of health information for quality and safety purposes and may impair access to information at the point of service. To the extent that state laws ultimately are determined to pose such problems, the House legislation would encourage further legislative consideration of federal law as a means of achieving ''commonality.''[27]

Indeed, a recently issued report by the GAO criticizes DHHS for not moving more quickly to create a national legal approach to privacy.[28] The report presumably buttresses the view of the congressional supporters of a national privacy standard. Yet both the congressional supporters and the GAO appear to presume the validity of the concerns expressed by representatives of various

---

bor regulations. *See* 71 Fed. Reg. at 45110 (anti-kickback safe harbors) and at 45140 (Stark exceptions) (Aug. 8, 2006), effective Oct. 10, 2006.

[19] *See* Sara Rosenbaum et al., ''The Legality of Collecting and Disclosing Patient Race and Ethnicity Data,'' The Robert Wood Johnson Foundation, 2006, available at http://www.healthinfolaw.org (Accessed Jan. 7, 2007).

[20] The Senate bill, ''Wired for Health Care Quality Act,'' was sponsored by Sen. Michael Enzi (R-Wyo.).

[21] The House bill, ''Health IT Promotion Act,'' was cosponsored by Rep. Nancy Johnson (R-Conn.) and Nathan Deal (D-Ga.). The bill was marked up by both the Committee on Ways and Means and the Committee on Energy and Commerce.

[22] *Health Information Technology: Hearing Before the House Comm. on Ways and Means*, Statement of the American College of Physicians, 109th Cong. (April 6, 2006); *Health Information Technology: Hearing Before the House Comm. on Ways and Means*, Statement of Don E. Detmer, M.D., president and chief executive officer of the American Medical Informatics Assn., 109th Cong. (July 27, 2005); *Health Information Technology: Hearing Before the House Comm. on Ways and Means*, Statement of Allen Weiss, M.D., president of Naples, Fla. Community Hospital Health Care Systems, 109th Cong. (July 27, 2005); *Health Information Technology: Hearing Before the Senate Commerce Comm.*, Statement of Peter Basch, M.D., 109th Cong. (June 30, 2005). Review of this testimony reflects the possibly widespread perception that HIPAA's preemption structure creates barriers to interoperability; yet despite the fact that this concern is frequently asserted, evidence to support the assertion has not been advanced. Similarly, a recent report by the Government Accountability Office (GAO) criticizes the DHHS for not moving more quickly to create a national legal approach to privacy, assuming, without citing any evidentiary support apart from the statements made by representatives of various interested parties, that the current system of a federal HIPAA privacy floor supplemented by state laws that are more stringent than HIPAA is a barrier to the creation of a nationwide interoperable system for heath information exchange. Government Accountability Office, ''Health Information Technology: Early Efforts Initiated by Comprehensive Privacy Approach Needed for National Strategy.'' GAO-07-238 (January 2007).

[23] S. 1418 § 4: ''Nothing in this title shall be construed to affect the scope or substance of . . . section 264 of the Health Insurance Portability and Accountability Act of 1996. . . .''

[24] S. 1418 § 2, as it passed the Senate, added a new Section 2903(c) to the Public Health Service Act (42 U.S.C. 201, et seq.).

[25] H.R. 4157 § 102(2), as it passed the House.

[26] H.R. 4157 § 205, as it passed the House.

[27] In recent years the United States Supreme Court has clarified Congress's powers under the commerce clause to establish uniform requirements related to health care practice. See *e.g., Gonzales v. Oregon*, 126 S. Ct. 904 (2006) (holding that although the Attorney General had exceeded his power in proscribing physician-assisted suicide under Oregon law, Congress does have the constitutional power to regulate the practice of medicine); *Gonzales v. Raich*, 545 U.S. 1 (2005), 125 S. Ct. 2195 (concluding that even though plaintiff's conduct was completely intra-state and involved state-sanctioned medical activities, the commerce clause nonetheless vests Congress with the power to reach purely personal and intra-state conduct). *See also* George J. Annas, ''Congress, Controlled Substances, and Physician-Assisted Suicide—Elephants in Mouseholes,'' *NEJM* 354 1079-1084 (March 6, 2006); Lawrence O. Gostin, POWER, DUTY, AND RESTRAINT. New York: Oxford University Press, 2003.

[28] Government Accountability Office, ''Health Information Technology: Early Efforts Initiated by Comprehensive Privacy Approach Needed for National Strategy.'' GAO-07-238 (January 2007).

  HCPR ISSN 1068-1213

interested parties that the current HIPAA preemption structure poses a barrier to the creation of a nationwide interoperable system for health information exchange, even though an evidentiary basis for this proposition has yet to be established.

Because of this congressional concern regarding the potential effects of more stringent state laws on the development of interoperable systems that also can produce a high and appropriate level of health information transparency, this project was undertaken. Its purpose was to analyze existing case law in the wake of the HIPAA statute and ensuing Privacy Rule, to determine the extent to which state privacy law may curtail the proper flow of PHI for quality and safety purposes.

Study Methods

This analysis involves a systematic review of all reported federal and state court cases decided between 1996 and 2006 involving the interpretation of state privacy law in relation to HIPAA. Although legal decisions are far from the only means of measuring the possible effects of law, judicial decisions represent a valuable window onto the world in two respects; first as a source of evidence about the existence of a problem, and second, as evidence of how the health care system understands the sources of powers and constraints within which it operates.[29]

Lawyers with extensive experience in health law generally, and HIPAA in particular,[30] undertook a legal scan of all reported federal and state court decisions in which the term ''HIPAA'' or ''Health Insurance Portability and Accountability Act'' or ''Health Insurance Portability and Accountability Act of 1996'' appeared. The scan was conducted utilizing standard legal research data bases and yielded 479 cases as of Nov. 21, 2006.

Each case that included any of these search terms at least once was then examined and categorized in accordance with a series of review criteria designed to determine the following: (a) the parties and the nature of the underlying dispute; (b) whether the dispute involved HIPAA preemption—that is, a conflict between the HIPAA disclosure standard and an arguably ''contrary'' or ''more stringent'' state law; and (c) whether the court addressed the ''merits'' of the HIPAA preemption claim (i.e. whether the court in fact had to determine if the state law was indeed ''contrary'' to or ''more stringent'' than the HIPAA disclosure standard).

The research team was especially interested in cases in which ''more stringent'' state laws may have prevented health care providers from obtaining access to patient information at the point of service. For purposes of our detailed analysis, the relevant cases were those that involved the allegation of a conflict between HIPAA and state law, thereby compelling a judicial preemption analysis. These cases then were assessed for their results, which were tabulated in the aggregate and further analyzed for their specific approach to the question of HIPAA preemption and state law.

A total of 479 cases fell within the scope of the analysis. The actual number of cases included in the subsequent preemption scan ultimately was reduced to 446 once duplication of decisions related to appeals and case consolidations were taken into account. Of these 446 cases, 333 were discarded because they raised no conflict between HIPAA and state law. Most of the discarded cases presented the question of HIPAA's constitutionality, whether HIPAA afforded individuals a private right of action to enforce HIPAA's protections,[31] or whether the secretary possessed the authority to promulgate the Privacy Rule. The remaining discarded cases addressed other sections of HIPAA not relevant to this analysis.

The remaining 113 cases, in which a potential conflict between HIPAA and state law was presented, then were categorized by the case domain, the underlying claim, the type of information sought, the types of entities involved, and whether the court concluded that state law, federal law, or both governed the dispute in light of the facts and the nature of the state law at issue.

Findings

The Key Characteristics of HIPAA Preemption Cases

In General

The single most important finding to emerge from this analysis is that to date, no HIPAA preemption case involves an effort by a health care provider to remove a state law barrier that is perceived as posing a barrier to access to or use of health information at the point of treatment. The implications and possible underlying reasons for this finding, which appears to contradict a central underlying assumption of the 2006 House legislation (i.e., the potential for state laws to act as legal barriers to provider access to patient safety and health care quality information), will be discussed in the Conclusion.

Second, of nearly equal importance, the underlying conflicts that appear to be driving disputes involving the relationship between state laws and the HIPAA privacy rule *appear to focus on the disgorgement of information as part of the legal process rather the use of information to improve quality, reduce disparities or create transparency*. That is, the principal *case domain* is a dispute regarding access to PHI as part of the legal process, rather than its use to advance quality and transparency. Indeed, because the operation of the legal system functions as the principal case domain, covered entities (including health care providers) are the most common party to the dispute; their most common posture is as defendants invoking the HIPAA Privacy Rule as a defense to a request for the disclosure of patient data in liability lawsuits brought against them. In a number of cases, health care providers may be in the position of plaintiffs attempting to secure access to PHI held by a non-patient third party.

Case Domains

The principal case domains are shown below in **Figure 1.**

Types of Underlying Claims

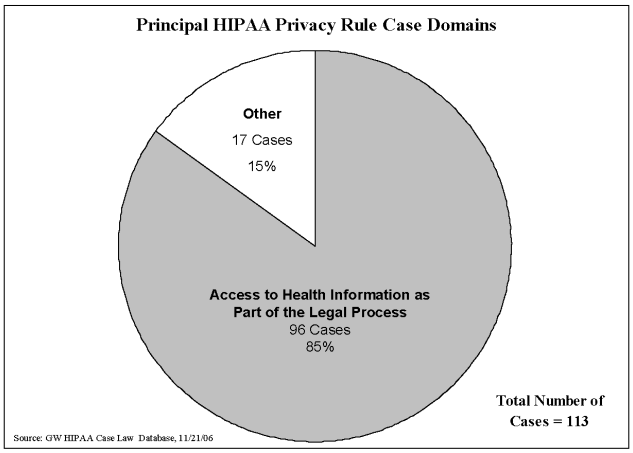
The relevant HIPAA cases concern many specific types of underlying claims that relate to the use or dis-

[29] William M. Sage, Judicial Opinions Involving Health Insurance Coverage: Trompe L'Oeil or Window on the World? 31 *Ind. Law Rev*. 4972 (1998).

[30] Professor Phyllis C. Borzi, one of the lawyers involved in this review, was under contract with the United States Department of Health and Human Services during 1999 and 2000, to assist in evaluating the public comments on the proposed Privacy Rule and examining policy and legal options that led to the promulgation of the final HIPAA rule in 2000.

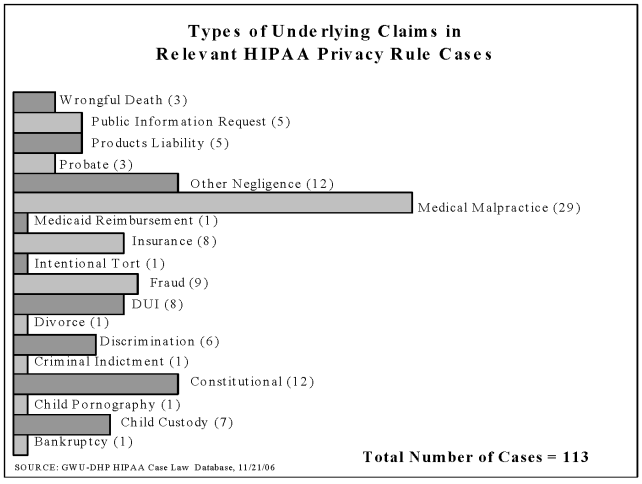
[31] HIPAA does not provide for a private right of action. *See Acara, supra* note 10.

Figure 1



closure of health information within the operation of the legal process. **Figure 2** underscores the rich array of legal claims in which access to health information is sought for a variety of reasons and becomes central to the dispute.

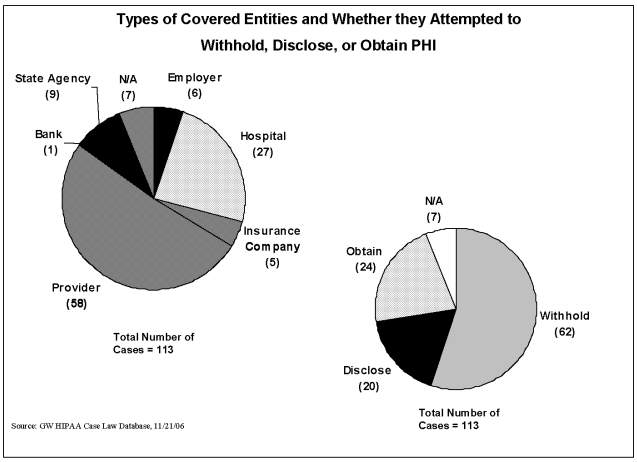
Figure 2



Types of Covered Entities Involved in HIPAA Preemption Cases

Because they possess the PHI at issue, or seek the PHI for defensive purposes in malpractice cases, covered entities always will be involved in the Privacy Rule cases in some capacity. Although not always an actual litigant in the dispute, the covered entity, at the very least, is awaiting judicial direction as to the disposition of the PHI it possesses. **Figure 3** illustrates both the types of covered entities holding the PHI at issue, as well as whether the covered entity is seeking to withhold, disclose, or obtain the PHI (for a malpractice defense). Consistent with our finding that the legal process is the principal domain for HIPAA preemption cases, **Figure 3** shows that the most common case scenario involves a health care provider attempting to shield information that he or she possess from legal access by the patient or a third party. The most common plaintiffs are not other providers attempting to secure access to health information for use at the point of care, but instead, private individuals, health insurers, providers defending against malpractice, or federal and state public agencies that seek information for reasons related to their underlying claims.

Figure 3



Types of Information Sought

Figure 4 illustrates the broad array of information or PHI that HIPAA cases may involve. By far, the most common type of information is the medical record itself, but often the information concerns evidence from non-treating physicians during the course of litigation, such as depositions and non-treating physician communications.

Careful reading of the preemption cases indicates that courts already are actively engaged in an effort to reconcile federal and state law in order to give life to the HIPAA legislative ''roadmap.''

The vast majority of HIPAA cases involve the operation of a state's legal process rather than efforts to improve health care quality through access to protected information.

The HIPAA preemption cases largely involve access to PHI as part of civil actions, through court-supervised discovery as well as part of government or insurance investigations. A fair number of cases also involve criminal prosecutions under state or federal law. HIPAA preemption analysis comes into play most directly as courts attempt to reconcile HIPAA's standards with state law standards related to the status and disclosure of evidence in legal proceedings; in other words, at its core, the typical preemption case involves the judicial determination of whether HIPAA alters state law standards governing the disclosure of PHI as part of the legal process.

For example, courts have concluded that HIPAA does not create a new federal substantive right that would protect PHI from disclosure in the normal course of business (i.e., does not create a new, federal physician/patient privilege). Instead, courts find that HIPAA's impact is to establish specific procedural steps that covered entities must follow in order to use and/or disclose PHI, or more typically, to justify withholding disclosure of such information.[32]

[32] *See In Re Grand Jury Proceedings,* 2006 WL 2831035 (D. Me. Oct. 3, 2006); *Abbott v. Texas Dept. of Mental Health and Mental Retardation*, 2006 WL 2504417 (Tex. App.-Austin Aug.

   ISSN 1068-1213

Judicial decisions involving HIPAA preemption essentially can be summarized as follows: notwithstanding the widely held perception that HIPAA creates federal disclosure barriers, HIPAA allows entities to set disclosure policies that advance health care quality and transparency and ensure conformance to state disclosure law. The court decisions underscore that not only do covered entities fail to use the flexibility they possess under HIPAA, but even more strikingly, that covered entities do not understand the practical operation of HIPAA.

A Closer Look at the HIPAA Preemption Decisions

In a typical case scenario, the covered entity holding PHI is confronted with a request or demand for PHI. The covered entity then faces three basic questions under the Privacy Rule: (1) must the PHI be disclosed; (2) may the PHI be disclosed; and (3) is disclosing the PHI prohibited?

Taken together, the decisions underscore the great degree of flexibility accorded covered entities under HIPAA where disclosure of PHI is concerned. **More importantly, our review of the existing HIPAA decisions underscores the absence of cases in which a more stringent state law stops a provider disclosure for patient care purposes.**

Interestingly, and particularly important for preemption purposes, a clear trend emerges in the cases toward reconciliation of state and federal law in order to avoid precisely the types of conflicts that would unduly burden data exchange. **Instead of treating HIPAA and state law as conflicting, the courts overwhelmingly interpret HIPAA so as to enable covered entities to comply with both bodies of law.**

HIPAA's rules for disclosure can be classified into two basic categories—required and permitted[33]—and as part of their preemption analysis, the courts focus on applying these two types of disclosures, even if the covered entity has ignored, or appears not to understand, them.

Figure 5 summarizes HIPAA's disclosure standards.

The HIPAA preemption cases, taken together, suggest that by far, the most confusing category of disclosures involve permitted disclosures which are ''required by law'' (these include disclosures of PHI required by a state or federal statute, regulation or by a court order). The confusion relates to the fact that *even though the disclosure is required by state law*, HIPAA permits the entity to decide whether it will comply with state law without first obtaining patient authorization. In other words, a covered entity has the power to invoke HIPAA's federal privacy floor to preempt a state statute mandating disclosure. As a matter of state law, disclosure is required. As a matter of HIPAA, disclosure is permissive.

HIPAA requires covered entities to adopt written policies and procedures as part of their compliance standards. [34] These policies must explain a covered entity's approach to permitted disclosures. In their decisions, courts do not dwell on (or typically even mention) whether the entity has in fact complied with this HIPAA requirement that the covered entity must have a written disclosure policy, instead they focus on whether the disclosure is required under HIPAA.

In reviewing the HIPAA preemption cases, we found *no* cases in which the demand for disclosure involved treatment or payment.

Instead, the cases involve disclosure demands related to the situations shown in **Figure 2 —** demands for information as part of the legal process. The cases involve

Figure 4

Type of Information Sought in HIPAA Cases	
911 tapes	1
Deposition of non-party treating physician	1
Ex-parte communication with non-party treating physician of the plaintiff	28
Financial records and tax returns of treating physicians	1
HIV status of a prisoner	1
Informed consent and participant questionnaires from participants in medical device clinical trials	1
Insurance records	2
Lead citations issued to property owners	1
Medicaid claims documents that include PHI	1
Medical information in employee personnel file	1
Medical record	52
Medicare billing and refund records	1
Mental hospital commitment records	1
Names and addresses of other patient-witnesses	5
Name, justification, type of coverage, and claims history for all people receiving city health benefits	1
Paramedic's testimony re defendant's statements made in the course of providing health care treatment	1
Patient scheduling information	2
Positive results of employee's drug test administered by employer state agency	1
Results of a compulsory medical exam for police officers	1
Statements made to nurses during the course of treatment	1
Statistics regarding allegations of patient abuse at state-run mental health facilities	1
Triage time, treatment time, and triage designations for non-party ER patients	1
NA	7
Total Cases	**113**

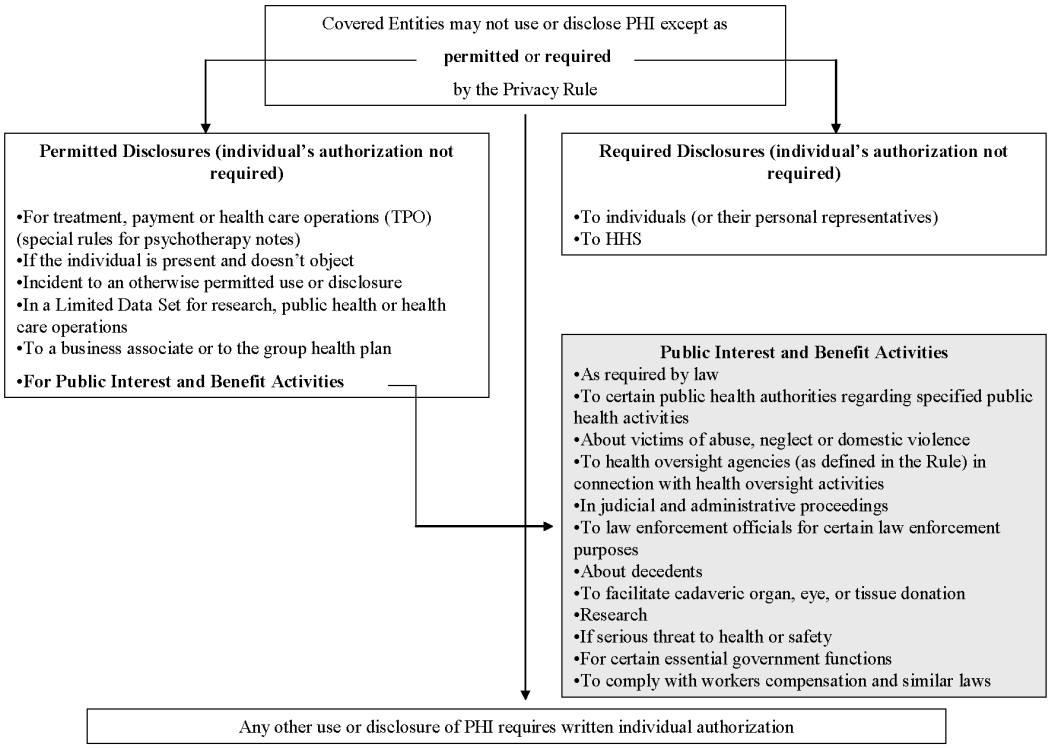
Source: GWU DHP HIPAA Case Law Database, 11/21/06

30, 2006); *Findley v. Findley*, 937 So.2d 912 (La. Ct. App. 2006); *Gendal v. Billotti*, 2006 WL 2135525 (N.Y. Sup. Ct. July 31, 2006); *State v. Siegel*, 136 P.3d 1214 (Or. Ct. App. June 16, 2006); *Bihm v. Bihm*, 932 So.2d 732 (La. Ct. App. 2006); *Boyd v. City and County of San Francisco*, 2006 WL 1390423 (N.D. Cal. May 18, 2006); *Sanders v. St. Charles Hosp. and Rehabilitation*, 820 N.Y.S.2d 846 (N.Y. Sup. Ct. 2006); *Richter v. Mutual of Omaha Ins. Co.*, 2006 WL 1277906 (E.D. Wis. May 5, 2006); *Anderson v. City of New York*, 2006 WL 1134117 (E.D.N.Y. April 28, 2006); *Rice v. Union Central Life Ins. Co.*, 2006 WL 1128223 (D. Idaho April 26, 2006); *Giangiulio v. Ingalls Memorial Hosp.*, 850 N.E.2d 249 (Ill. App. 2006); *Rosales v. City of Bakersfield*, 2006 WL 988605 (E.D. Cal. April 13, 2006); *Armstrong v. Commonwealth of Kentucky*, 2006 WL 1045709 (Ky. Ct. App. March 31, 2006); *State ex rel. Cincinnati Enquirer v. Daniels*, 844 N.E.2d 1181 (Ohio 2006); *In re Stuart G.*, 820 N.Y.S.2d 426 (N.Y. Co. Ct. 2006); *Sunrise Opportunities, Inc. v. Regier*, 2006 WL 581150 (N.D. Ill. March 7, 2006); *Massaro v. Massaro*, 2006 WL 350065 (N.J. Super. App. Div. Feb. 17, 2006).

[33] 45 CFR § 164.502(a) et seq.

[34] 45 CFR § 164.530(i)(1).

Figure 5
HIPAA Privacy Structure



demands for information under a state or federal law, in which a determination must be made as to whether HIPAA permits, requires, or prohibits the disclosure. Even though the disclosure of PHI in the particular situation at issue may be ''required by law,'' under HIPAA's structure, the disclosure remains permissive with the covered entity.[35] Virtually every case we examined involved a permitted disclosure under HIPAA, thus illustrating the little-acknowledged fact that HIPAA leaves covered entities with enormous control over information flow, even in legal disclosure cases.

Practically speaking, however, while HIPAA may appear to allow covered entities to decide whether or not they will comply with other requirements of law because HIPAA classifies the ''required by law'' disclosure as permitted, in reality, covered entities that ignore state law requirements do so at their peril. Perhaps it would have been more sensible for the secretary in crafting the HIPAA Privacy Rule to classify these legally required disclosures as ''required,'' but the courts have approached this conundrum by simply noting that nothing in HIPAA precludes the covered entity from complying with both HIPAA and state law. And in most instances, the court leaves the decision of how to reconcile any potential problem with the covered entity, rather than ordering the covered entity to take a particular action.

Ironically perhaps, most of the cases involved health care professionals and institutions that, as covered entities, attempted either to block a disclosure or to secure disclosure from other covered entities in situations *not* involving either treatment or payment. Thus, the heart of the judicial analysis becomes whether HIPAA allows a health care provider to shield the information, even though the relevant state or federal law under which the information is sought is one couched in ''required by law'' terms. The fact that HIPAA's most common use may be by covered entities attempting to shield information is somewhat ironic in view of concern on the part of some policymakers that HIPAA's tolerance of state privacy law would prevent providers from securing information critical to treatment decisions.

Thus, it would appear that HIPAA's most important contribution to the flow of personal health information may lie in the fact that HIPAA empowers covered entities to withhold information whose disclosure previously would have been required by law. In these cases, the HIPAA privacy ''floor'' effectively ensures that, at a covered entity's election, HIPAA can be used to create a shield that can withstand state legal disclosure statutes. Put another way, the overwhelming majority of HIPAA preemption cases involve efforts to reconcile the HIPAA privacy floor with ''contrary'' state statutes that require *disclosure,* rather than efforts to reconcile HIPAA's privacy floor with ''more stringent'' state privacy laws. HIPAA gives covered entities a great deal of power to determine whether they will comply with state disclosure statutes, and covered entities have the power to determine if they will conform their disclosure policies to the laws of the state in which they operate. In these cases, rather than ordering a disclosure, the courts simply point out that the covered entity in question faces no

[35] As previously noted, the covered entity must adopt policies and procedures regarding permitted disclosures, including which permitted disclosures it will allow and under what circumstances. Despite this HIPAA requirement, the courts have yet to penalize covered entities for failure to adopt a policy. Instead, the courts seem to assume that all permitted disclosures allowed under HIPAA apply to all requests for PHI.

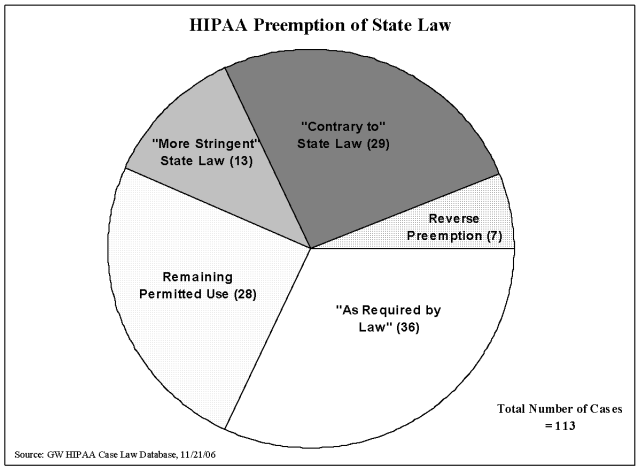
   ISSN 1068-1213

barrier in complying with the state law, thereby reconciling the HIPAA floor with state disclosure law.[36]

Courts rarely find HIPAA preemption of state laws that are "contrary to" the HIPAA privacy floor and instead focus on the discretionary power of covered entities to disclose information.

The heart of a HIPAA preemption analysis is a determination of whether state law is ''contrary to'' HIPAA and thus preempted, or whether the state law is ''saved'' (in ERISA parlance) because it is ''more stringent'' than the HIPAA floor.[37] **Figure 6** underscores how few cases actually involve either of these two categories. Only 13 of the 113 cases reviewed involved judicial consideration of allegedly ''more stringent'' state law.

Figure 6



[36] *See Abbott v. Texas Dept. of Mental Health and Mental Retardation*, 2006 WL 2504417 (Tex. App.-Austin Aug. 30, 2006); *Sanders v. St. Charles Hosp. and Rehabilitation*, 820 N.Y.S.2d 846 (N.Y. Sup. Ct. 2006); *Anderson v. City of New York*, 2006 WL 1134117 (E.D.N.Y. April 28, 2006); *Rosales v. City of Bakersfield*, 2006 WL 988605 (E.D. Cal. April 13, 2006); *Armstrong v. Commonwealth of Kentucky*, 2006 WL 1045709 (Ky. Ct. App. March 31, 2006); *State ex rel. Cincinnati Enquirer v. Daniels*, 844 N.E.2d 1181 (Ohio 2006); *Massaro v. Massaro*, 2006 WL 350065 (N.J. Super. App. Div. Feb. 17, 2006); *Clancey v. Paramount Pictures Corp.*, 2005 WL 2222193 (Cal. Ct. App. Sept. 14, 2005); *In re Involuntary Termination of Parent Child Relationship of A.H., L.H., C.H., and J.H*, 832 N.E.2d 563 (Ind. Ct. App. 2005); *Raynor v. St. Vincent's Hosp. and Medical Center*, 801 N.Y.S.2d 241 (N.Y. Sup. Ct. 2005); *Ohio Legal Rights Service v. Buckeye Ranch, Inc.*, 365 F. Supp.2d 877 (S.D. Ohio April 2005).

[37] On its Web site, DHHS's Office for Civil Rights (OCR), which is charged with interpreting and administering HIPAA's Privacy Rule, describes in both its summary of the Rule and in its Frequently Asked Questions what it means for a state law to be ''more stringent'' than HIPAA. For instance, Question #405 explains that the Privacy Rule establishes a floor of federal protections and that if state law provides greater privacy protections for patients, state law is not preempted, even if it would appear to be ''contrary to'' HIPAA. Among the examples cited by OCR are those involving state laws prohibiting disclosure of an individual's HIV status. Although HIPAA permits such disclosure in certain circumstances, OCR says there is no onflict between the state law and HIPAA and therefore no preemption of state law because the ''more stringent'' state law would prevail.

Twenty-nine cases[38] have squarely addressed the question of whether a state law is preempted by HIPAA. Of most significance are those cases dealing with discovery disputes about what type of information can be used in a trial.

For example, when state laws require individuals who file a malpractice action to execute a broad release of their personal medical records upon filing, some courts have held that such laws are ''contrary to'' HIPAA and thus preempted because HIPAA includes a very specific and detailed list of requirements that must be included in any valid authorization for the release of PHI to a third party.[39] These cases generally stand for the proposition that HIPAA's more protective patient authorization requirements will govern in the face of sweeping state laws that mandate broad release of personal health information in a malpractice litigation context.

A related set of cases deals with state laws that address the informal *ex-parte* communications of defense counsel with plaintiff's treating physicians who are not themselves involved in the malpractice litigation. Some courts have determined that such contact is not allowed because HIPAA is more restrictive;[40] other courts have

[38] *See Hulse v. Suburban Mobile Home Supply Company*, 2006 WL 2927519 (D. Kan. Oct. 12, 2006); *Griffin v. Burden*, 2006 WL 2567223 (Ga. Ct. App. Sept. 7, 2006); *Crisp Regional Hosp., Inc. v. Sanders*, 2006 WL 2507153 (Ga. Ct. App. Aug. 31, 2006); *Brazier v. Crockett Hosp.*, 2006 WL 2040408 (Tenn. Ct. App. July 20, 2006); *Allen v. Wright*, 2006 WL 1976762 (Ga. Ct. App. July 14, 2006); *Northlake Medical Center, LLC v. Queen*, 634 S.E.2d 486 (Ga. Ct. App. 2006); *Constantino v. North Shore University Hosp.*, 820 N.Y.S.2d 842 (N.Y. Sup. Ct. 2006); *Fisher v. Yale University*, 2006 WL 1075035 (Conn. Super. Ct. April 3, 2006); *State v. Downs*, 923 So.2d 726 (La. Ct. App. 2005); *Harmon v. Maury County, TN*, 2005 WL 2133697 (M.D. Tenn. Aug. 31, 2005); *Travis v. Thane International, Inc.*, 2005 WL 1971900, (M.D. Tenn. Aug. 15, 2005); *Michelson v. Wyatt*, 880 A.2d 458 (N.J. Super. App. Div. 2005); *Alsip v. Johnson City Medical Center*, 2005 WL 1536192 (Tenn. Ct. App. June 30, 2005); *In re Diet Drug Litigation*, 895 A.2d 493 (N.J. Super. Ct. Law Div. 2005); *Valli v. Viviani*, 801 N.Y.S.2d 243 (N.Y. Sup. Ct. 2005); *Croskey v. BMW of North America, Inc.*, 2005 WL 1959452 (E.D. Mich. Feb. 16, 2005.); *Bayne v. Provost*, 359 F. Supp.2d 234 (N.D.N.Y. 2005); *Creely v. Genesis Health Ventures, Inc.*, 2004 WL 2943661 (E.D. Pa. Dec. 17, 2004); *Keshecki v. St. Vincent's Medical Center*, 785 N.Y.S2d 300 (N.Y. Sup. Ct. 2004); *Hawes v. Golden*, 2004 WL 2244448 (Ohio Ct. App. Sept. 22, 2004); *Crenshaw v. Mony Life Insurance Co.*, 318 F. Supp.2d 1015 (S.D. Ca. 2004); *Law v. Zuckerman*, 307 F. Supp.2d 705 (D. Md. 2004); *Smith v. American Home Products Corp. Wyeth-Ayerst Pharmaceutical*, 855 A.2d 608 (N.J. Sup. Ct. 2003); *Tapp v. State*, 108 S.W.3d 459 (Tex. Ct. App.-Houston 2003); *U.S. ex re. Stewart v. Louisiana Clinic*, 2002 WL 31819130 (E.D. La. December 12, 2002); *O'Donnell v. Blue Cross Blue Shield of Wyoming*, 173 F. Supp.2d 1176 (D. Wyo. 2001); *Cowan v. Combined Ins. Co. of America*, 67 F. Supp.2d 1312 (M.D. Ala. 1999); *M.P. Means v. Independent Life and Accident Insurance Co.*, 963 F. Supp. 1131 (M.D. Ala. 1997); *Wright v. Combined Insurance Co. of America*, 959 F. Supp. 356 (N.D. Miss. 1997).

[39] *See Griffin v. Burden*, 2006 WL 2567223 (Ga.App. Sept. 7, 2006); *Crisp Regional Hosp., Inc. v. Sanders*, 2006 WL 2507153 (Ga.App. August 31, 2006); *Allen v. Wright*, 2006 WL 1976762 (Ga.App. July 14. 2006); *Northlake Medical Center, LLC v. Queen*, 2006 WL 1914716 (Ga.App. July 13, 2006). *See* 45 CFR § 164.508(b) for the HIPAA requirements for a valid authorization.

[40] *See Allen v. Wright*, 2006 WL 1976762 (Ga.App. July 14, 2006); *Travis v. Thane International, Inc.*, 2005 WL 1971900,

determined that the practice may continue because a covered entity (the physicians) can comply with both the state law and HIPAA.[41] In those latter cases, the court may order the non-party treating physician to disclose PHI with certain restrictions (since it would be a permitted disclosure under HIPAA for participation in legal proceedings), even though the physician, as a HIPAA-covered entity, may not have adopted a policy regarding such disclosure. Alternatively, the court simply may remind the non-party physician that disclosure of PHI in this context is permitted under HIPAA, and leave it to the physician to determine whether or not to communicate with defense counsel.[42]

Courts permit "more stringent" state laws to survive preemption.

In only13 [43] out of the 113 cases has the issue been whether a state law is ''more stringent'' than HIPAA and thus capable of surviving preemption. Again, most of these cases arise in the discovery context and focus on whether certain PHI—usually found in the patient's medical record—is admissible at trial. In some cases, the covered entity holding PHI may want to introduce the medical record in defense of a malpractice claim; in others, the covered entity wants to avoid producing PHI in the court proceeding, arguing that production violates the state physician/patient privilege law. Some courts have held that state laws governing the physician/patient privilege are ''more stringent'' than HIPAA and thus can be enforced because they override the HIPAA permitted use provisions.[44] In other cases, however, the courts have concluded that the more stringent state law can live in harmony with HIPAA.[45] In these cases, courts, rather than counseling the covered entity holding PHI to adopt a disclosure policy permitting the disclosure, simply shift the decision of whether or not to disclose back to the covered entity or alternatively, issue an order directing disclosure.

The "as required by law" cases illustrate how the courts are reconciling the HIPAA privacy floor with state disclosure laws.

Thirty-six cases have addressed what happens when a covered entity seeks to disclose (or is asked to disclose) PHI pursuant to a law other than HIPAA, under HIPAA's ''as required by law'' permitted use.[46] These cases also illustrate the means by which courts conclude that both state laws and HIPAA can co-exist. For requests for public information, some courts have held the covered entity may disclose PHI pursuant to a state

---

(M.D.Tenn. Aug. 15, 2005) (although court did allow admittance of this evidence because the patient had authorized it); *Alsip v. Johnson City Medical Center*, 2005 WL 1536192 (Tenn.Ct.App. June 30, 2005); *Croskey v. BMW of North America, Inc*., 2005 WL 1959452 (E.D. Mich. Feb. 16, 2005); *Bayne v. Provost*, 359 F. Supp.2d 234 (N.D.N.Y. 2005); *Keshecki v. St. Vincent's Medical Center*, 785 N.Y.S2d 300 (NY Sup. Ct. 2004); *Crenshaw v. Mony Life Insurance Co*., 318 F. Supp.2d 1015 (S.D. Ca. 2004); *Law v. Zuckerman*, 307 F. Supp.2d 705 (D. Md. 2004).

[41] *See Hulse v. Suburban Mobile Home Supply Co.*, 2006 WL 2927519 (D. Kansas Oct. 12, 2006); *In re Diet Drug Litigation*, 895 A.2d 493 (N.J.Super.L. 2005); *Valli v. Viviani*, 801 N.Y.S.2d 243 (N.Y.Sup. 2005); *Smith v. American Home Products Corp. Wyeth-Ayerst Pharmaceutical*, 855 A.2d 608 (NJ Sup. Ct 2003).

[42] *See Hitchcock v. Suddaby*, 801 N.Y.S.2d 234 (N.Y. Sup. Ct. 2005); *Keshecki v. St. Vincent's Medical Center*, 785 N.Y.S2d 300 (N.Y. Sup. Ct. 2004).

[43] *See Findley v. Findley*, 937 So.2d 912 (La. Ct. App. 2006); *Bihm v. Bihm*, 932 So.2d 732 (La. Ct. App. 2006); *QT, Inc. v. Mayo Clinic Jacksonville*, 2006 WL 1371426 (N.D. Ill. May 15, 2006); *Giangiulio v. Ingalls Memorial Hosp.*, 850 N.E.2d 249 (Ill. App. 2006); *Ottinger v. Mausner*, 816 N.Y.S.2d 698 (N.Y. Sup. Ct. 2006); *Grove v. Northeast Ohio Nephrology Assoc., Inc.*, 844 N.E.2d 400 (Ohio Ct. App. 2005); *Citizens for Health v. Leavitt*, 428 F.3d 167 (3rd Cir. 2005); *Belote v. Strange*, 2005 WL 2758007 (Mich. Ct. App. Oct. 25, 2005); *In re Berg*, 886 A.2d 980 (N.H. 2005); *Y.J.K. v. D.A.*, 2005 WL 2220021 (D.C. Super. Ct. Sept. 9, 2005); *Moss v. Amira*, 826 N.E.2d 1001 (Ill. App. Ct. 2005); *Michota v. Bayfront Medical Center, Inc.*, 2005 WL 900771 (Fla. Cir. Ct. Feb. 24, 2005); *United States v. Diabetes Treatment Centers of America*, 2004 WL 2009416 (D. D.C. May 17, 2004).

[44] *See Giangiulio v. Ingalls Memorial Hosp*., 850 N.E.2d 249 (Ill.App. 2006); *Bihm v. Bihm*, 2006 WL 1479802 (La.App. 3 Cir. May 31, 2006); *Ottinger v. Mausner*, 816 N.Y.S.2d 698 (N.Y.Sup. 2006); *Grove v. Northeast Ohio Nephrology Assoc., Inc*., 844 N.E.2d 400 (Ohio App. 9 Dist. 2005); *Y.J.K. v. D.A*., 2005 WL 2220021 (D.C. Super. Sept. 9, 2005).

[45] *See Findley v. Findley*, 2006 WL 2393129 (La.App. Aug. 16, 2006); *Belote v. Strange*, 2005 WL 2758007 (Mich.App. Oct. 25, 2005); *In re Berg*, 886 A.2d 980 (N.H. 2005); *Moss v. Amira*, 826 N.E.2d 1001 (Ill.App.2005).

[46] *See Abbott v. Texas Dept. of Mental Health and Mental Retardation*, 2006 WL 2504417 (Tex. App.-Austin August 30, 2006); *State v. Siegel*, 136 P.3d 1214 (Or. Ct. App. June 16, 2006); *Boyd v. City and County of San Francisco*, 2006 WL 1390423 (N.D. Cal. May 18, 2006); *Rodriguez v. Folksamerica Reinsurance Co.*, 2006 WL 1359119 (D. Conn. May 15, 2006); *Sanders v. St. Charles Hosp. and Rehabilitation*, 820 N.Y.S.2d 846 (N.Y. Sup. Ct. 2006); *Richter v. Mutual of Omaha Ins. Co.*, 2006 WL 1277906 (E.D. Wis. May 5, 2006); *Anderson v. City of New York*, 2006 WL 1134117 (E.D.N.Y. April 28, 2006); *Rice v. Union Central Life Ins. Co.*, 2006 WL 1128223 (D. Idaho April 26, 2006); *Coffie v. City of Chicago*, 2006 WL 1069132 (N.D. Ill. April 21, 2006); *Rosales v. City of Bakersfield*, 2006 WL 988605 (E.D. Cal. April 13, 2006); *Armstrong v. Commonwealth of Kentucky*, 2006 WL 1045709 (Ky. Ct. App. March 31, 2006); *State ex rel. Cincinnati Enquirer v. Daniels*, 844 N.E.2d 1181 (Ohio 2006); *Massaro v. Massaro*, 2006 WL 350065 (N.J. Super. App. Div. Feb. 17, 2006); *U.S. v. Zamora*, 408 F. Supp.2d 295, 298 (S.D.Tex. 2006); *Protection & Advocacy System, Inc. v. Freudenthal*, 412 F. Supp.2d 1211 (D. Wyo. 2006); *In re Estate of Broderick*, 125 P.3d 564 (Kan. Ct. App. 2005); *U.S. v. W. R. Grace*, 401 F. Supp.2d 1093 (D. Mont. 2005); *U.S. ex rel. Kaplan v. Metropolitan Ambulance & First-Aid Corp.*, 395 F. Supp.2d 1 (E.D.N.Y. 2005); *Clancey v. Paramount Pictures Corp.*, 2005 WL 2222193 (Cal. Ct. App. Sept. 14, 2005); *Tomczak v. Ingalls Memorial Hosp.*, 834 N.E.2d 549 (Ill. App. Ct. 2005); *In re Involuntary Termination of Parent Child Relationship of A.H., L.H., C.H., and J.H*, 832 N.E.2d 563 (Ind. Ct. App. 2005); *In re MacLeman*, 808 N.Y.S.2d 918 (N.Y. Sur. Ct. 2005); *U.S. v. Mathis*, 377 F. Supp.2d 640 (M.D.Tenn. 2005); *Commonwealth v. Pratt*, 2005 WL 1459650 (Mass. Super. Ct. June 9, 2005); *Carpenter v. Massachusetts Inst. of Technology*, 2005 WL 1476542 (Mass. Super. Ct. May 12, 2005); *Hitchcock v. Suddaby*, 801 N.Y.S.2d 234 (N.Y. Sup. Ct. 2005); *Raynor v. St. Vincent's Hosp. and Medical Center*, 801 N.Y.S.2d 241 (N.Y. Sup. Ct. 2005); *Fliegelman v. Stamford Health System, Inc.*, 2005 WL 1273887 (Conn. Super. Ct. April 27, 2005); *Ohio Legal Rights Service v. Buckeye Ranch, Inc.*, 365 F. Supp.2d 877 (S.D. Ohio April 2005); *Chapman v. Health and Hospitals Corporations*, 796 N.Y.S.2d 876 (N.Y. Sup. Ct. 2005); *Smith v. Rafalin*, 800 N.Y.S.2d 357 (N.Y. Sup. Ct. 2005); *Webdale v. North General Hosp.*, 796 N.Y.S.2d 861 (N.Y. Sup. Ct. 2005); *McGuire v. Rawlings Co.*, LLC. 2005 WL 895870 (Conn. Super. Ct. March 14, 2005); *Girard v. Girard*, 2005 WL 704366 (Conn. Super. Ct. February 10, 2005); *Steele v. Clifton Springs Hosp. and Clinic*, 788 N.Y.S.2d 587 (N.Y. Sup. Ct. 2005); *In re Will of Ettinger*, 793 N.Y.S.2d 739 (N.Y. Sur. Ct. 2005).

   ISSN 1068-1213

Freedom of Information Act (FOIA) request and that HIPAA does not present a bar to disclosure.[47] However, when the state law itself prohibits disclosure through an exception to its FOIA, both HIPAA and the state law operate together to deny the release of PHI.[48] HIPAA has not been an obstacle to disclosure under state mandatory disclosure laws, since this form of compliance is permitted under several HIPAA provisions.[49]

The majority of cases that deal with the ''as required by law'' test permit disclosure under HIPAA. These cases serve to illustrate the frequency with which covered entities may simply be unsure about what to do in the face of a court order, subpoena, or other discovery request when PHI is sought to be used at trial as evidence. Inevitably, the party seeking to use the information to its benefit argues that the covered entity may release PHI pursuant to HIPAA's ''as required by law'' provisions for use in ''judicial or administrative proceedings'' or for ''law enforcement purposes.'' Courts generally have held in these situations that the covered entity may disclose the PHI under this permitted use, so long as the HIPAA safeguards—such as notice to the patient and an accompanying protective order limiting the release—are in place and there exists no more stringent state law on the issue.[50]

Courts view HIPAA as creating a disclosure protocol for PHI, not a substantive physician/patient privilege.

As noted, the courts are consistent in their view that HIPAA did not create a federal physician/patient privilege, and most are in agreement that HIPAA generally creates a process for determining legal uses and disclosures of PHI, not substantive evidentiary rights.[51] These conclusions have led some courts, in evaluating the legal effect of HIPAA preemption, to confront the following question: in a federal case involving federal claims brought in federal court pursuant to the federal rules of evidence, must ''more stringent'' state evidentiary laws apply in a solely federal context as a result of the HIPAA preemption rule? Termed ''reverse preemption'' by the courts, a clear trend is emerging that denies applicability of state evidentiary laws even if arguably more stringent than HIPAA, when the suit involves enforcement of federal law. As one court described it, ''the HIPAA regulations do not impose state evidentiary privileges on suits to enforce federal law.''[52] The cases further illustrate judicial reconciliation of HIPAA with other law, both state and federal: stricter state laws will be applicable in state cases while HIPAA will apply without interference from state evidentiary law in the federal domain.

Conclusion

This analysis explores how the legal system grapples with the introduction of federal rules governing the protection, management, and disclosure of personal health information. Nearly 500 cases related to HIPAA have been litigated since its enactment, and 113 of these cases focus on the important question of how HIPAA's federal standards are to be squared with both state law and with other federal laws. Only 13 cases involve reconciling the HIPAA disclosure provisions with more stringent state laws. Most cases involve the application of HIPAA and state privacy laws to the question of PHI in the legal process. **There is no evidence from the case law that either HIPAA or state privacy laws act as barriers either to the disclosure of health information essential to health care quality or to the use of such information to create transparent health care quality information through aggregated and de-identified health information.**

The sheer volume of litigation focusing on HIPAA's interface with the legal process probably will come as no surprise to those who are familiar with the legal process or HIPAA. Health care is a field driven by law and adversarial proceedings. Health information is and always has been a basic byproduct and pillar of health care and health information is integral to the legal process. Because the disposition of countless claims turns on the consideration of medical evidence—much of it ''PHI'' as the term is used in HIPAA—litigation involving the meaning of HIPAA in relation to state law is inevitable.

A close examination of the 113 HIPAA Privacy Rule cases decided as of the end of 2006 in which decisions on the merits were reached supports several basic conclusions:

First, the cases overwhelmingly focus on HIPAA's effect on the use of PHI in the legal process itself. Few cases present conflicts between HIPAA and more stringent state laws. None of the cases involve the impact of more stringent state laws on efforts by health care providers to secure information essential for treating patients. Indeed, a common litigation posture is that of provider as a covered entity attempting to use HIPAA as either a sword or a shield: either to prevent disclosure of PHI or to gain access to it to defend against malpractice. In either scenario, the analysis is the same: can state law be reconciled with HIPAA's permitted disclosure provisions?

Second, examination of the judicial process at work in the HIPAA cases underscores a clear desire on the part of the courts to reconcile state disclosure laws with HIPAA privacy safeguards. Ironically, the key to reconciling HIPAA and state law is that in most of the cases, the disclosure at issue is one that is permitted, but not

[47] *See Abbott v. Texas Dept. of Mental Health and Mental Retardation*, 2006 WL 2504417 (Tex.App.-Austin Aug. 30, 2006); *State ex rel. Cincinnati Enquirer v. Daniels*, 844 N.E.2d 1181 (Ohio 2006).

[48] *See Hill v. East Baton Rouge Parish Dept. of Emergency Medical Services*, 925 So.2d 17 (La.App. 1 Cir. 2005); *Michelson v. Wyatt*, 880 A.2d 458 (N.J.Super.A.D. 2005).

[49] *See Protection & Advocacy System, Inc. v. Freudenthal*, 412 F. Supp.2d 1211 (D.Wyo. 2006).

[50] *See Boyd v. City and County of San Francisco*, 2006 WL 1390423 (N.D.Cal. May 18, 2006); *Rodriguez v. Folksamerica Reinsurance Co.*, 2006 WL 1359119 (D.Conn. May 15, 2006); *Anderson v. City of New York*, 2006 WL 1134117 (E.D.N.Y. April 28, 2006); *Rice v. Union Central Life Ins. Co*., 2006 WL 1128223 (D.Idaho April 26, 2006); *Rosales v. City of Bakersfield*, 2006 WL 988605 (E.D.Cal. April 13, 2006).

[51] See *Shemonic v. Manoff*, 2006 WL 741447 (S.D.Ill. March 21, 2006); *Holzle v. Healthcare Services Group, Inc*., 801 N.Y.S.2d 234 (N.Y.Sup. 2005); *Northwestern Mem'l Hosp. v. Ashcroft*, 362 F.3d 923, 925 (7th Cir. 2004).

[52] *Northwestern Mem'l Hosp. v. Ashcroft*, 362 F.3d 923, 925 (7th Cir. 2004); *See also In re Grand Jury Proceedings*, 2006 WL 2831035 (D. Me. Oct. 3, 2006); *Sunrise Opportunities, Inc. v. Regier*, 2006 WL 581150 (N.D.Ill. March 7, 2006); *U.S. ex rel. Camillo v. Ancilla Systems, Inc*., 233 F.R.D. 520 (S.D.Ill. 2005); *Kalinoski v. Evans*, 377 F. Supp.2d 136, 139 (D.D.C. 2005); *EEOC v. Boston Market Corp.*, 2004 WL 3327264 (E.D.N.Y. Dec. 16, 2004); *National Abortion Federation v. Ashcroft*, 2004 WL 555701 (S.D.N.Y. March 19, 2004).

required, under HIPAA. Covered entities have the power under HIPAA—through their adoption of explicit disclosure policies—to determine the circumstances and extent of disclosure, including arguably the extent to which they will comply with variable state disclosure laws (although, as previously noted, a decision by the covered entity not to comply with a state law requirement is undertaken at the entity's peril).

If anything, HIPAA—far from being undermined by the continued vitality of more stringent state laws—permits covered entities to substitute their own uniform policies for variable state disclosure laws. If covered entities desire to disclose the requested PHI, they generally can do so either by adopting a disclosure policy that permits disclosure, by observing a state reporting requirement, or by exercising an exception to a state privilege law. Based on the cases under HIPAA to date, covered entities that do not want to disclose information stand an excellent chance of persuading a court that HIPAA classifies most disclosures as permitted and therefore, the decision to disclose is up to the entity. Whether covered entities understand their power to determine health information transparency and establish such norms is doubtful at this point, given the extensive litigation seeking clarification of duties and rights under HIPAA.

Third, courts are consistent in their view that HIPAA creates no new substantive evidentiary rights but instead sets up a process for managing and disclosing PHI, a process that centralizes decisionmaking within the covered entity itself as part of the Privacy Rule's permitted disclosure provisions. Moreover, courts appear to dismiss the relevance of state evidentiary law as a means of processing the disclosure and management of PHI when the issue is one arising under federal law and the judicial forum is federal.

Fourth, were Congress to attempt to legislate uniformity in health information law, many of the most important applications of these changes would come in the context of states' legal processes, not in a health care quality or information transparency context. In this vein, more compelling policy development would appear to be initiatives aimed at fostering the diffusion of the technology essential to the adoption and use of health information systems capable of routinely providing the public with vital information about the quality and safety of care.

Based on our review of the HIPAA privacy cases, we find nothing to suggest that the preservation of more stringent state laws creates a barrier to interoperability of HIT systems that can produce public information about system performance. Indeed, if anything, the current HIPAA privacy standard may confer on covered entities greater power to shield information than might be desirable in an age of health information transparency. Courts understand HIPAA as vesting covered entities with the power to determine the extent of PHI disclosure under state law, even state laws whose disclosure obligations are compelled by overarching public health policy concerns (such as disclosures of PHI related to a public health threat and during a time of public health emergency declared under state law).[53] Whether HIPAA could be invoked to prevent a state from pursuing affirmative information transparency efforts using de-identified and aggregated data remains to be seen.

To the extent that there is the potential for more stringent state laws to limit access to PHI essential to safety and quality, such a barrier is not evident in the HIPAA litigation to date. One explanation is that there are few state laws that meet the ''more stringent than'' test, thereby suggesting that such wide variability is more myth than reality. Another is that where state law in fact is more stringent, providers are aware of the law and thus routinely do not seek the information. This custom of avoiding certain health information because consent is required poses a serious problem for health care quality improvement.

A key step to clarify the fact that neither HIPAA nor state laws pose barriers to health care quality improvement or transparency systems would be comprehensive guidance from the HHS Office for Civil rights explaining HIPAA's relevance to such initiatives and how compliance can be achieved. States that set independent privacy laws might consider undertaking parallel efforts to clarify the legality of health information use as part of transparency and quality improvement initiatives.

Were Congress to consider the legal option of further expanding HIPAA preemption to substitute uniform federal standards for those more stringent state laws that do exist, such a legal approach to uniformity would raise several important implications.

First, Congress would be required to revisit the very difficult question of privacy of personally identifiable health information that would compel a substantive balancing of intensely held personal health interests against broader questions of public health and welfare. Although this balancing of personal versus public considerations is a traditional feature of the lawmaking process, the question of whether to undertake an effort to set a HIPAA ceiling, as well as a HIPAA floor, is a complicated one. HIPAA already preempts state disclosure laws to establish a federal privacy floor. Given the extremely limited evidence of a negative impact that the existence of more stringent state laws has had, the policy question is whether there is a justification for undertaking a strenuous effort to set a privacy ceiling, especially when the issues that would need to be addressed involve some of the most personal in all of health care and are inextricably linked to the functioning of state civil and criminal judicial process.

Second, it is not clear that a broadening of HIPAA preemption would limit legal uncertainty and litigation. Were Congress to adopt a ''field preemption'' approach, that is, to preempt all state health information law, the result would be continuing judicial involvement and uncertainty. While this approach has been urged by some as part of the debate over the pending health information systems legislation, no greater clarity or reduction in litigation is likely to result from such a change because the courts still will be involved in HIPAA cases. Broad field preemption in the privacy arena requires statutory language preempting state laws that ''relate to'' health information privacy to achieve the goal of establishing a single uniform standard for the management and disclosure of PHI. Even limiting preemption to those state laws ''connected with'' privacy, confidentiality, or security would not eliminate the potential for

[53] In addition, in cases of national emergency, the Project BioShield Act of 2004, Pub. L. No. 108-276 (July 21, 2004), 118 STAT. 835, authorizes the HHS secretary to suspend certain provisions of HIPAA.

   ISSN 1068-1213

ever-expanding litigation, since, as this review of HIPAA preemption cases illustrates, it is not the merits of underlying state privacy laws that are at issue, but rather, disputes regarding state laws that have precisely the opposite purpose, i.e., to compel the disclosure of PHI as part of the legal process and the operation of state judicial systems. That Congress would desire to entrench itself more deeply in the state legal process seems unlikely.

For a sobering example of how difficult it is to craft a federal law that would eliminate or drastically reduce uncertainty and litigation by preempting state law, one only needs to look at the example of the broad preemption that Congress adopted in the Employee Retirement Income Security Act of 1974 (ERISA). In ERISA § 514, Congress set out to preempt all state laws that ''relate to'' employee benefit plans covered by ERISA, except those regulating insurance, banking, and securities. In the more than three decades since ERISA's enactment, considerable litigation over the meaning of ERISA's preemption clause has occurred, and yet we still do not know with certainty the extent of permissible state health regulation. More than 20 ERISA preemption cases have traveled to the Supreme Court alone, and as Justice David Souter so aptly described the problem in one of those cases, as a practical matter, everything ''relates to'' everything else.[54]

As Congress and the administration move forward to encourage the acceleration of electronic health information systems, removing legal barriers to adoption is clearly important. However, identifying these barriers and determining how best to remove or minimize them requires careful examination of the factual and operational basis for concern, as well as the potential impact of various alternative solutions. Although this review suggests that the current HIPAA preemption standard does not pose a barrier to provider access to treatment information through interoperable systems, important challenges do remain, chiefly where reconciling HIPAA with other *federal* laws is concerned, particularly privacy laws related to federal health care financing programs such as Medicaid (whose own privacy statute has yet to be conformed to the modern expectations of HIPAA), as well as privacy standards relevant to certain forms of federally funded treatment, such as treatment for substance abuse.

Study Limitations

Several limitations with respect to this analysis should be noted. First, we considered only reported cases in which there was a decision on the merits of the applicability of the HIPAA Privacy Rule, including preemption. Anecdotally, we have heard of instances in which a provider sought information from another covered entity holding PHI for treatment purposes but was unable to obtain it. Since HIPAA expressly permits such disclosures, we presume that these types of conflicts may be relatively few and tend to get resolved between the covered entities involved.

Second, we did not examine the underlying state laws themselves to identify the full range of laws that might fall into the ''more stringent'' test. Indeed, we have concerns that such an examination might prove futile, since many state laws that turn out to be more stringent than HIPAA may arise, not in the context of privacy or confidentiality statutes, but in a legal process or evidentiary context, or some other context wholly unrelated to the substance of health information privacy itself.

Although this review of the HIPAA privacy cases, particularly those that focus on preemption, does not support the argument that HIPAA preemption poses a barrier to HIT interoperability, by providing policymakers with an accurate picture of the legal landscape under HIPAA, a more thorough examination of the potential trade-offs between electronic health information systems and privacy protections for individuals becomes possible.

[54] *New York State Conference of Blue Cross & Blue Shield Plans v. Travelers Ins. Co.*, 514 U.S. 645, 656 (1995) (''If 'relate to' were taken to extend to the furthest stretch of its indeterminacy, then for all practical purposes pre-emption would never run its course, for '[r]eally, universally, relations stop nowhere,' H. James, Roderick Hudson xli (New York ed., World's Classics 1980)'').