Bottom-Up or Top-Down? Removing the Privacy Law Obstacles to Healthcare Reform in the National Healthcare Crisis

JOHN W. HILL,* ARLEN W. LANGVARDT** & JONATHAN E. RINEHART***

The nation is faced with a healthcare crisis of monumental proportions that threatens the economic stability of the nation and raises moral issues of healthcare quality and availability.[1] Politicians rant about healthcare reform, but often this ranting may reflect more political posturing than efficacy in the solutions proposed.[2] Amid the rancor, one of the most underdiscussed facets of the crisis is that of the legal obstacles that need to be removed if the nation is to enjoy the full benefits of a true national healthcare system, as opposed to the current patchwork of local systems cobbled together by a morass of operational and legal cords.[3] Indeed, the U.S. healthcare system has been analogized to a modern airliner flown with biplane controls in terms of its diagnostic and treatment capabilities versus its administrative and clinical operations.[4] In terms of its cost, politics, quality, and efficiency, healthcare is no longer a state and local issue but rather a national one,[5] and one that threatens the U.S. economy.[6] Continuing with the aircraft analogy, it is as if air traffic is being governed by state laws—with each state having a somewhat different set of rules—some of which prohibit flying across state lines. We argue that both the quality of future treatment and its cost depend to a significant extent upon rationalizing laws that govern

---

* Arthur M. Weimer Chair, Professor of Accounting and Life Sciences Fellow, Center for the Business of Life Sciences, Kelley School of Business, Indiana University.

** Professor of Business Law and Life Sciences Fellow, Center for the Business of Life Sciences, Kelley School of Business, Indiana University.

*** J.D. Candidate, 2010, Indiana University Maurer School of Law — Bloomington; M.B.A. Candidate, 2010, Kelley School of Business, Indiana University.

1. *See, e.g.*, U.S. GEN. ACCOUNTING OFFICE, No. GAO-04-793SP, COMPTROLLER GENERAL'S FORUM: HEALTHCARE 3 (2004), *available at* http://www.gao.gov/cgi-bin/getrpt?GAO-04-793SP [hereinafter HEALTHCARE FORUM] (stating that the public and private sectors are facing major challenges with respect to cost, access, and quality of healthcare).

2. *See* Paul Krugman & Robin Wells, *The Healthcare Crisis and What to Do About It*, N.Y. REV. OF BOOKS, Mar. 23, 2006, *available at* http://www.nybooks.com/articles/18802 (book review).

3. *See generally* John W. Hill, Arlen W. Langvardt & Anne P. Massey, *Law, Information Technology, and Medical Errors: Toward a National Healthcare Information Network Approach to Improving Patient Care and Reducing Malpractice Costs*, 2007 U. ILL. J.L. TECH. & POL'Y 159, 236–37 (examining the current state of the national healthcare system and some of the legal issues attending a move toward a national health information network).

4. *See* Roy L. Simpson, *Medical Errors, Airplanes, and Information Technology*, NURSING MGMT., June 2000, at 14.

5. *See* Sharon R. Klein & William L. Manning, *Telemedicine and the Law*, HEALTH L. RESOURCE, http://www.netreach.net/~wmanning/telmedar.htm. For a discussion of the failure of the legal and regulatory environment to keep up with changes in distributive medicine, see *id.*

6. Diana Manos, *GAO: Healthcare Costs Threaten to Undo American Economy*, HEALTHCARE FIN. NEWS Jan. 31, 2008, *available at* http://www.healthcarefinancenews.com/printStory.cms?id=7603.

healthcare. One of the most critical bodies of these laws—because of the tradeoffs between patients' rights to privacy and clinical interoperability—is that pertaining to the privacy of personal healthcare information.[7]

Current national political policy seems to favor a bottom-up solution in which state legal regimes gradually evolve to permit some sort of electronically connected national healthcare network—or perhaps the lesser objective of a collection of loosely linked local and regional networks. If this national network is to evolve rapidly, a patchwork of federal and state privacy laws that promise to seriously impede this network must somehow be harmonized in order to resolve systemic problems related to quality, inefficiency, and inaccessibility.[8] As described in the following part, the U.S. healthcare system suffers from serious problems related to quality, access, and affordability, which affect most Americans in one or more ways. Removing the barriers to a national healthcare network is one of the most important aspects of resolving this healthcare crisis—hence the need for harmonization of disparate privacy laws. This suggests the following questions: Is it possible for such harmonization to take place bottom-up? Conversely, is a top-down solution needed in which a national legal framework for healthcare is forged, either through preemptive federal legislation or by providing federal incentives to encourage states to adopt model legislation and harmonize their disparate privacy laws? We briefly explore these questions, suggesting possible answers and weighing their potential effectiveness. First, we address the current state of domestic healthcare with its myriad problems and deficiencies and consider why there is a need for a national healthcare network together with a corresponding legal framework that will permit such a network to thrive. Second, we review some of the more important laws and legal issues that attend privacy law. Third, we discuss proposed model legislation and its potential efficacy in forging a coherent, national framework for healthcare information privacy. We conclude by offering several observations regarding the various prescriptions for rationalizing healthcare privacy laws.

I. THE STATE OF THE U.S. HEALTHCARE SYSTEM

Constituting over sixteen percent of the nation's gross domestic product and representing its largest industry,[9] the $1.9 trillion U.S. healthcare system[10] is a contrarian paradox of massive proportions in that the world's best treatment capabilities—capabilities growing rapidly with advances in molecular medicine[11]—are exacerbating its difficulties with quality, accessibility, and cost.[12] Expressed somewhat

---

7. *See* Hill et al., *supra* note 3, at 188–93, 226–27.

8. *See id.* at 200–01, 230–33. For discussion of the lack of national healthcare information connectivity and ensuing problems, see *id.* at 197–200, 202–04.

9. David Stires, *Technology Has Transformed the VA*, FORTUNE, May 15, 2006, at 131, *available at* http://money.cnn.com/magazines/fortune/fortune_archive/2006/05/15/8376846/index.htm.

10. Richard Hillestad, James Bigelow, Anthony Bower, Federico Girosi, Robin Meili, Richard Scoville & Roger Taylor, *Can Electronic Medical Record Systems Transform Healthcare? Potential Health Benefits, Savings, and Costs*, 24 HEALTH AFF. 1103, 1103 (2005).

11. *See* Hill et al., *supra* note 3, at 161–62, 206–07.

12. *E.g.*, Krugman & Wells, *supra* note 2; *see also* David W. Bates, Mark Ebell, Edward

differently, as healthcare technology becomes better and people live longer and have more medical issues, the potential for both medical errors and the cost of cutting-edge treatment increase, making accessibility less affordable.[13] The circularity inherent in this paradox makes finding efficacious solutions to the problem difficult and portends even more debate among the various players, including politicians, healthcare providers (HCPs), health insurers, and pharmaceutical companies among others, all of whom have vested interests of one form or the other as well as ideological biases.[14] As if this were not gloomy enough, problems of circularity extend beyond the better-treatment-leads-to-more-treatment paradox to more microlevel facets of the crisis. For example, collection of clinical outcome data is essential for building a high-quality, efficient healthcare system.[15] The difficulty is not just that the mechanisms for collecting such data are for the most part not in place; it is also that the patchwork of state healthcare data privacy laws layered on top of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA)[16] represent a huge obstacle to large-scale patient screening and treatment, physician performance, and tracking of outcomes,[17] despite some recent attempts at legal reforms.[18]

From a quality standpoint, there is near universal agreement that serious problems exist. In 2000, the Institute of Medicine issued a report indicating that as many as 98,000 patients are killed annually by medical errors,[19] and the United States lags behind some other first-world nations in several health treatment outcome measures.[20] Although there is disagreement as to the causes, there is also widespread consensus that the U.S. healthcare system is inefficient.[21] From an information technology standpoint, the U.S. healthcare industry has been described as "arguably the world's largest, most inefficient information enterprise."[22] From an accessibility standpoint, despite an abundance of political rhetoric,[23] there remains high variance in the rates at

---

Gotlieb, John Zapp & H.C. Mullins, *A Proposal for Electronic Medical Records in U.S. Primary Care*, 10 J. AM. MED. INFORMATICS ASS'N 1, 4 (2003) (stating that the "unaided human mind simply cannot process the current volume of clinical data required for practice," that "[a]s information becomes obsolete, it is not refreshed, and new knowledge cannot be integrated," and that "[t]he advent of genomics will only make this problem worse").

13. *E.g.*, Krugman & Wells, *supra* note 2. This contrarian paradox has been described rather succinctly by two distinguished Harvard professors, one of whom is a former U.S. Surgeon General: "[I]t was the very progress which physicians had made in science, which involved them in new difficulties in the practice of their art." JULIUS B. RICHMOND & RASHI FEIN, THE HEALTH CARE MESS: HOW WE GOT INTO IT AND WHAT IT WILL TAKE TO GET OUT 40 (2005) (citation omitted).

14. *Id.* at 1, 6–7.

15. HEALTHCARE FORUM, *supra* note 1, at 20.

16. 42 U.S.C. §§ 1320d-1 to -8 (2000).

17. *See* Hill et al., *supra* note 3, at 193, 226–33.

18. *See id.* at 221–26, 229–35 (detailing the problems that remain after these attempts).

19. INST. OF MED., TO ERR IS HUMAN: BUILDING A SAFER HEALTH SYSTEM 26, 31 (Linda T. Kohn, Janet M. Corrigan & Molla S. Donaldson eds., 2000), *available at* http://www.nap.edu/openbook/0309068371/html/R1.html.

20. HEALTHCARE FORUM, *supra* note 1, at 7.

21. *See, e.g.*, Krugman & Wells, *supra* note 2.

22. Hillestad et al., *supra* note 10, at 1103.

23. David J. Brailer, Digital Medicine in the Era of Health Reform, Keynote Address at Harvard Medical School Seminar: Patient-Centered Computing and eHealth: Transforming

which geographically diverse patients obtain healthcare, with no adequate clinical explanation for this variance.[24] From a financial perspective, the healthcare crisis is said to actually be a triple crisis: (1) the unraveling of traditional, employer-based health insurance; (2) a growing problem in Medicaid, a state-administered, federally funded healthcare program that provides healthcare for many uninsured patients; and (3) a federal budget crisis in which healthcare spending is growing faster than per capita income.[25] As employers are increasingly unable or unwilling to fund employer-sponsored programs, the costs of which are growing faster than corporate profits, more of the cost of healthcare has fallen upon the government.[26] As a result the U.S. Comptroller General estimates that government healthcare payments as a percentage of gross domestic product will more than triple by 2070.[27]

Two important and closely linked keys to healthcare reform are improved clinical interoperability and health information exchange.[28] Many of the current clinical and administrative processes that characterize healthcare are like cart paths that have been paved over to make roads.[29] Mistake-proofing—"the use of process or design features to prevent errors or the negative impact of errors"—is an area that shows tremendous promise in improving healthcare quality and efficiency.[30] Although mistake-proofing can involve quite simple processes, more sophisticated technologies (e.g., bar coding, computerized physician order entry, and robotic pharmacies) are required to realize the full potential for reducing medical errors and the growing cost burden of healthcare.[31]

These technologies, and even more sophisticated ones, must be supported by health information systems that permit a reasonably free flow of patient information to HCPs.[32] Consequently, such systems are a second key to healthcare reform and an extension of process improvement. Once processes have been streamlined and mistake-proofed, they should be connected in a manner not unlike the cockpit of a modern jet fighter with, computer-integrated control system—as opposed to manual biplane

---

Healthcare Quality, (Mar. 29, 2008) (notes on file with authors).

24. HEALTHCARE FORUM, *supra* note 1, at 19. For one theory behind this disparity, see *id.* at 10–11.

25. Krugman & Wells, *supra* note 2.

26. *See* HEALTHCARE FORUM, *supra* note 1, at 6.

27. *See id.* at 5.

28. *See, e.g.*, Hill et al., *supra* note 3, at 209 (citing evidence from Evanston Northwestern Healthcare that improvements in clinical processes and health information technology need to go hand-in-hand).

29. This was underscored by Ronald W. Dollens, former CEO of Guidant Corp., who commented that fundamental process change was a prerequisite for healthcare improvement and successful, large-scale IT implementation within healthcare. Interview with Ronald W. Dollens, former President and CEO, Guidant Corp., and past Chairman, Healthcare Leadership Council, in Bloomington, Ind. (Feb. 1, 2006) (notes on file with authors).

30. JOHN GROUT, U.S. DEP'T OF HEALTH AND HUMAN SERVS., AHRQ PUB. NO. 07-0020, MISTAKE-PROOFING THE DESIGN OF HEALTH CARE PROCESSES 1 (2007).

31. *Id.* at 15. For extensive examination of the role that enhanced use of electronic medical records and other significant technologies may play in a new type of medical malpractice "reform"—a reform that focuses on the reduction of medical errors—see Hill et al., *supra* note 3, at 165–87, 194–97, 202–10.

32. *See* Hill et al., *supra* note 3, at 194–210 (arguing for national health electronic connectivity); *see also* GROUT, *supra* note 30, at 131 (discussing the need to conform to federal privacy laws in disclosing patient status).

controls—so that information flows seamlessly among HCPs and computers play a substantially greater role in aiding the medical treatment processes.[33] The penultimate state of such a system of controls would be a national health information network (NHIN) in which HCPs are linked electronically, the benefits of which include error reduction through system safeguards, interstate electronic healthcare, complete patient health information on demand regardless of location, and intensive, large-scale data collection that greatly facilitates medical research.[34]

Among the many factors that complicate healthcare reform are two that bear directly upon clinical interoperability and health information exchange. The first is the movement from a patient-centric model of treatment to one that is consumer-centric,[35] a dynamic that could impact the balance between patients' privacy concerns and their desires to play an active role in managing their health. Much of the public has a deep yearning to exercise more control over their health and sees healthcare information as the path that leads to better health.[36] This yearning is translating into a desire by patients to exert more control over treatment and have greater access to information about healthcare availability, quality, and cost.[37] This trend toward consumer-centric treatment may well lead to a greater interest on the part of consumers in ensuring that HCPs have the most current and complete personal health information possible, even at an increased risk of inadvertent disclosure of private information. Underscoring this trend is a greater willingness on the part of healthcare consumers to travel across state lines to save money or obtain better quality healthcare and a desire that HCPs exchange clinical information and provide patients with access to their medical records via the Internet.[38]

A second factor that bears upon improved clinical interoperability and health information exchange is a web of state and federal privacy laws that has evolved in a rather haphazard fashion. In some cases, these privacy laws require disparate levels of responsibility and diligence. In other cases, there is an outright conflict. In still others, they contain vagaries that leave HCPs wondering where permissible boundaries rest.[39] These laws are impeding healthcare consumers' ability to obtain high-quality care at an affordable cost,[40] and their rationalization is a necessary prerequisite for a true national healthcare system characterized by seamless interoperability and information

---

33. *See* Sarah Rubenstein, *Next Step Toward Digitized Health Records*, WALL ST. J., May 9, 2005, at B1; *see also* Hill et al., *supra* note 3, at 162 (discussing the role of computerization in health informatics and noting that the current state of medical record keeping has been described as largely a paper-and-pencil operation).

34. *See* Hill et al., *supra* note 3, at 204–10.

35. *See* DELOITTE CTR. FOR HEALTH SOLUTIONS, 2008 SUMMARY OF HEALTH CARE CONSUMERS: EXECUTIVE SUMMARY 20 (2008), *available at* http://www.deloitte.com/dtt/cda/doc/content/us_chs_ConsumerSurveyExecutiveSummary_200208.pdf.

36. Brailer, *supra* note 23.

37. *See* DELOITTE CTR. FOR HEALTH SOLUTIONS, *supra* note 35, at 20.

38. *Id.* at 22.

39. *See, e.g.*, Cheryl S. Camin, *HIPAA: To Preempt or Not to Preempt? That Is the Question (Especially in Litigation)*, ABA HEALTH ESOURCE, Sept. 2005, http://www.abanet.org/health/esource/vol2no1/camin.html.

40. *See* Hill et al., *supra* note 3, at 230–33.

exchange.[41] The next section briefly discusses some of the more important aspects of federal and state privacy laws as a foundation for a subsequent examination of the issues that attend their rationalization.

II. LEGAL ISSUES ATTENDING PATIENT PRIVACY: FEDERAL AND STATE LAWS

Healthcare providers (HCPs) are generally classified as the legal owners of the medical records regarding their patients,[42] with many states also providing patients a statutory or common law right of access to the records that contain information about them.[43] The usual status of HCPs as owners of the records, however, does not give them free rein to disclose the records' content to third parties. Medical ethics codes offer general guidance on the disclosure issue by providing that, when a physician acquires information about a patient, the physician has an ethical duty to avoid disclosing the information to third parties except when furnishing care to the patient necessitates disclosure or when disclosure advances important societal interests.[44]

Although many states have enacted laws that restrict HCPs from revealing the contents of medical records to third parties,[45] the statutes vary concerning the range of HCPs subject to them,[46] the types of disclosures prohibited, and the patient's private right of enforcement (if any).[47] These helped set the stage for federal action to establish a national rule, though, as will be seen, the national rule that was adopted does not necessarily preempt state laws.[48]

The federal government's foray into the medical information privacy realm resulted in the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[49] and regulations promulgated pursuant to it. For the most part, HIPAA delegated to the Department of Health and Human Services (HHS) the authority to adopt standards for HIPAA-specified entities to follow in protecting, using, and disclosing patients' medical information.[50] Congress listed the following entities as subject to the to-be-developed HHS standards: "health plan[s]," "health care clearinghouse[s]," and "health

---

41. *Id*. at 236–37.

42. JAMES WALKER SMITH, HOSPITAL LIABILITY § 14.04[2] (2005); *see* JOINT COMM'N ON ACCREDITATION OF HOSPS., ACCREDITATION MANUAL FOR HOSPITALS 93 (1985).

43. SMITH, *supra* note 42, § 14.04[2]. The federal Privacy Act speaks to the right of access issue in a limited sense by establishing that patients may inspect medical records maintained about them by federal agencies, including federal hospitals. 5 U.S.C. § 552a (2006).

44. DEAN M. HARRIS, CONTEMPORARY ISSUES IN HEALTHCARE LAW AND ETHICS 102, 107 (2d ed. 2003). Hospitals and healthcare workers other than physicians hold this same ethical obligation. SMITH, *supra* note 42, § 14.04[1].

45. *See* HARRIS, *supra* note 44, at 104.

46. *See id.*

47. *See id.* at 104–07; *see also* Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 654 (2002).

48. *See* HARRIS, *supra* note 44, at 104.

49. 42 U.S.C. §§ 1320d-1 to -8 (2000).

50. *Id.* §§ 1320d-1 to -3. In addition, HIPAA directed HHS to develop standards under which covered entities would be expected to utilize safeguards to preserve the accuracy and confidentiality of patients' health information. *Id.* § 1320d-2(d)(2).

care provider[s] who transmit[] any health information in electronic form" in connection with specified financial and administrative transactions.[51]

After identifying the covered entities and outlining general guidelines, HIPAA assigned HHS the job of crafting most of the details.[52] HHS then promulgated regulations that, in this Article, will be referred to collectively as the "Privacy Rule."[53] The Privacy Rule establishes the specific obligations imposed on covered entities concerning the safeguarding of *protected health information* (PHI). According to the Privacy Rule, PHI is medical information that is "individually identifiable" as pertaining to a certain patient.[54] "[I]ndividually identifiable information" includes health information that "(1) is maintained in any form or medium, (2) relates to, identifies, or could identify the person that the health information concerns, and (3) is transmitted or maintained by a covered entity."[55]

To the greatest extent reasonably possible, covered entities must keep PHI confidential.[56] This general duty notwithstanding, the Privacy Rule recognizes various purposes that make PHI disclosure lawful if the covered entities comply with a "minimum necessary" standard when making the disclosure.[57] Perhaps most

---

51. *Id.* § 1320d-1(a). HIPAA's *health plan* definition includes health insurance offered by private insurers, medical coverage furnished by health maintenance organizations, and governmental healthcare programs such as Medicare and Medicaid. *Id.* § 1320d(5). A *healthcare clearinghouse* is an entity—public or private—that obtains patients' medical information in the course of insurance claims processing or in similar contexts. *Id.* § 1320d(2); SMITH, *supra* note 42, § 14.04[3]. HIPAA gave a somewhat broad definition to *healthcare provider*. Any "provider of medical or other health services [as defined in other federal statutes], and any other person furnishing health care services or supplies" is considered a healthcare provider for purposes of HIPAA. 42 U.S.C. § 1320d(3). This means that physicians, nurses, dentists, pharmacists, hospitals, and clinics are subject to HIPAA and the related regulations if those parties "transmit[] any health information in electronic form" in regard to administrative or financial transactions. 42 U.S.C. § 1320d-1(a).

52. 42 U.S.C. §§ 1320d-1 to -3.

53. 45 C.F.R. §§ 160.101–160.552, 164.102–50164.34 (2007).

54. 45 C.F.R. § 160.103.

55. *Id.*; *see also* 42 U.S.C. § 1320d(6) (providing definition of individually identifiable health information). Without question, this definition covers much information typically contained in medical records. When medical information is not "individually identifiable," it is not PHI and thus is not subject to the Privacy Rule's general prohibition against disclosure. *See* 45 C.F.R. § 164.501. "De-identification" of medical information—through removal of names, addresses, telephone numbers, social security numbers, and other facts tending to identify a particular patient—keeps the information from being PHI. *Id.* § 164.514; *see* SMITH, *supra* note 42, § 14.04[3].

56. *See* 42 U.S.C. § 1320d-2(d)(2); 45 C.F.R. §§ 164.502, 164.514.

57. 45 C.F.R. §§ 164.502, 164.514. The "minimum necessary" standard receives further discussion *infra* notes 62–63 and accompanying text. An important related obligation imposed on covered entities applies to their dealings with "business associates," which are outside parties that receive PHI during the performance of important services for covered entities. 45 C.F.R. § 160.103. Accounting, law, and consulting firms would be examples of business associates. *See id.*; SMITH, *supra* note 42, § 14.04[3]. The Privacy Rule provides that a covered entity may lawfully disclose PHI to a business associate only if the covered entity receives satisfactory written assurances that the business associate will safeguard the information. 45 C.F.R. § 164.502(e). This obligation applies regardless of whether the disclosure required the patient's

importantly, a covered entity's disclosure of PHI is generally permissible without any need to obtain the patient's consent if the disclosure is for purposes of "treatment, payment, or healthcare operations."[58] HCPs, health plans, and healthcare clearinghouses thus have significant latitude to disclose PHI during key day-to-day operations.[59] The Privacy Rule recognizes a number of other purposes for which covered entities may disclose PHI without first allowing the patient a chance to object.[60] In other instances, however, the patient must provide consent before disclosure of PHI may lawfully occur.[61]

If a covered entity discloses PHI for a permissible purpose, the entity must also satisfy the "minimum necessary" standard, which limits the amount of information that may be disclosed.[62] The amount of PHI disclosed must not exceed the amount reasonably necessary to accomplish the purpose of the disclosure. Therefore, the patient's full medical record may not be disclosed if only certain information in the record pertains to the purpose of the disclosure.[63]

To increase patients' awareness of their HIPAA rights, the Privacy Rule requires covered entities to furnish patients a written notice of those rights.[64] The notice must mention the previously described instances in which their PHI may be disclosed—not only those instances in which the patient's consent is necessary, but also those in which

---

consent or was for a purpose that eliminated the need for the patient's consent. *See id.* In addition, such assurances are necessary if the business associate is authorized to receive or create PHI on the covered entity's behalf. *Id.* § 164.502(e)(1). If a covered entity acquires knowledge that a business associate has violated the privacy-preservation obligation on a repeated basis, the covered entity must remedy the violations or sever ties with the business associate. *Id.* § 164.504(e)(1)(ii).

58. *See* 45 C.F.R. § 164.506. The Privacy Rule extends different treatment to psychotherapy notes, however. If the PHI includes psychotherapy notes, the patient must provide consent in order for the covered entity to disclose the notes lawfully—even if the disclosure would be for the otherwise permissible purposes of treatment, payment, or healthcare operations. *Id*. § 164.508.

59. *See id.* § 164.506.

60. *See id.* § 164.512. These purposes are: to make disclosures required by law; to further public health activities such as compiling records regarding deaths, births, and disease incidents; to provide information about abuse or domestic violence victims; to aid in health oversight activities; to fulfill duties in legal proceedings; to further law enforcement purposes; to provide information about deceased persons; to assist with organ donation programs; to advance research purposes; to guard against significant threats to public health or safety; to aid military operations and other specialized government functions; and to provide information relevant to workers' compensation matters. *Id.* § 164.512(a)(l).

61. *Id.* § 164.510. If a covered entity will be disclosing PHI for purposes other than those noted in this section of the Article, patient consent will normally be required. *See id.* § 164.502(a).

62. *Id.* § 164.502(b); *see also* SMITH, *supra* note 42, § 14.04[3][c]. The "minimum necessary" standard controls regardless of whether the disclosure is one for which the patient's consent is required or, instead, is one for which the Privacy Rule eliminates the need for the patient's consent. *See* 45 C.F.R. § 164.502.

63. SMITH, *supra* note 42, § 14.04[3][c]. The Privacy Rule underscores the importance of the "minimum necessary" standard by instructing covered entities to develop standard-implementing policies and procedures. *See* 45 C.F.R. § 164.514(d).

64. 45 C.F.R. § 164.520.

the patient's approval is not a prerequisite.[65] The Privacy Rule further requires covered entities to inform the patient of her right to request that her PHI not be disclosed for certain purposes and in particular settings. "Request" is a key word here, because a covered entity need not honor the patient's nondisclosure request if the Privacy Rule otherwise allows the making of such a disclosure.[66]

Under the Privacy Rule, patients have a right of access to their PHI—a right that includes an entitlement to inspect and copy a "designated record set."[67] *Designated record set* is defined as a group of "medical records and billing records about individuals maintained by or for a covered healthcare provider[,]" a health plan's "enrollment, payment, claims adjudication, and case or medical management records systems[,]" or records "[u]sed . . . by or for the covered entity to make decisions about individuals."[68]

Although patients have substantial rights under HIPAA and the Privacy Rule, patients cannot sue covered entities that commit violations. Instead, HHS and the Department of Justice (DOJ) have enforcement authority.[69] Patients may complain about alleged violations to HHS, which may then investigate and initiate civil administrative proceedings if they seem warranted.[70] The Privacy Rule provides HHS a power it has utilized with frequency: the power to resolve complaints informally. In informal resolutions, HHS obtains assurances from the covered entity that the alleged problem will be resolved and not repeated.[71] If the case goes through full administrative proceedings[72] and violations are found, the violators may be assessed civil penalties of not more than $100 per violation.[73] Even when a violation is proven,

---

65. *Id.* The notice must also inform the patient of her right to inspect her PHI and request amendments to it or corrections in it. The patient must be informed in the notice that she may request an accounting of instances in which her PHI was disclosed to third parties. *Id.* §§ 164.520(b), 164.528; s*ee id.* §§ 164.524, 164.526; SMITH, *supra* note 42, § 14.04[3][c][vi]. In addition, the notice must inform patients of how they may lodge complaints about PHI disclosures that they believe were improper. 45 C.F.R. § 164.520(b)(1)(vi). Covered entities must designate a person to receive patients' complaints about possible violations and must document all such complaints. *Id.* § 164.530(a)(1)(ii). In addition, covered entities must designate a privacy officer who oversees the entity's policies and procedures for maintaining confidentiality of PHI. *Id.* § 164.530(a)(1)(i). HHS has also adopted related regulations that require covered entities to utilize specific security measures to safeguard PHI when it is electronically transmitted and used. *See id.* §§ 164.306, 164.308, 164.312.

66. 45 C.F.R. § 164.522; *see also id.* § 164.506.

67. *Id.* § 164.524(a).

68. *Id.* § 164.501. Electronic medical records systems, of course, are subject to the patient's right of access to the same extent that paper records systems are. *See id.*

69. 42 U.S.C. § 1320d-6 (2000); 45 C.F.R. § 160.306(a).

70. 45 C.F.R. § 160.306(a), (c).

71. *See id.* §§ 160.312, 160.416; *see also* Rob Stein, *Medical Privacy Law Nets No Fines*, WASH. POST, June 5, 2006, at A1 (noting that during the first three years of privacy protections put in place by HIPAA and the Privacy Rule (the period of 2003 through 2006), HHS almost always engaged in informal resolution when patients filed grievances).

72. *See generally* 45 C.F.R. §§ 160.300–160.316, 160.400–160.426.

73. 42 U.S.C. § 1320d-5(a); 45 C.F.R. § 160.404(b)(1)(i). HIPAA and the Privacy Rule also establish a $25,000 cap on the total civil penalties imposed on a covered entity for all of its violations of the same requirement or prohibition during the same calendar year. 42 U.S.C. §

however, HHS has the authority to waive the civil penalty.[74] Besides outlining the potential civil consequences for violations of HIPAA and the Privacy Rule, HIPAA contains a criminal liability provision that outlaws the knowing disclosure or acquisition of individually identifiable health information in violation of the statute and the Privacy Rule.[75]

Since the Privacy Rule took effect, the civil and criminal penalties established in HIPAA and detailed in the Privacy Rule have essentially gone unused. As of June 2006, HHS had imposed no civil penalties.[76] As to roughly 14,000 complaints made by patients, HHS found no violation, resolved the matter informally, or found a violation but declined to impose a civil penalty.[77] HHS's clear preference thus far has been to resolve complaints of civil violations informally and to encourage voluntary compliance on the part of covered entities.[78] Concerning HIPAA's criminal provision, little activity has occurred. Although HHS had referred approximately 300 cases to the DOJ for possible criminal prosecution as of June 2006, the DOJ had instituted only two actual prosecutions.[79]

As might be expected, covered entities have preferred HHS's strategy of encouraging voluntary compliance to holding full administrative proceedings and imposing civil penalties. Privacy advocates, however, have reacted differently, seeing HHS's disinclination to impose civil penalties as a signal to covered entities that they can take a lax approach to fulfilling the duties established in HIPAA and the Privacy Rule.[80] If the use of electronic medical records becomes more prevalent, this debate would seem likely to assume added significance.

HIPAA and the Privacy Rule generally supersede state laws that directly contradict the federal requirements for safeguarding PHI[81] or that furnish less protection for

---

1320d-5(a); 45 C.F.R. § 160.404(b)(1)(ii).

74. 45 C.F.R. § 160.412. HIPAA provides that no civil penalty is to be imposed if a criminal violation is established. 42 U.S.C. § 1320d-5(b). The criminal liability provision, *id.* § 1320d-6, will be discussed below. *See infra* note 75. HIPAA also provides that no civil penalty is to be imposed if the violator neither knew, nor had reason to know, of the violation, assuming the failure to comply with the Privacy Rule either stemmed from "reasonable cause and not . . . willful neglect" or was corrected promptly by the violator. 42 U.S.C. § 1320d-5(b).

75. 42 U.S.C. § 1320d-6(a). A criminal violation may lead to a fine of up to $50,000 and a maximum of one year of imprisonment. If the violation consists of disclosing or obtaining individually identifiable health information "under false pretenses," the maximum fine and term of imprisonment increase to $100,000 and five years, respectively. *Id.* § 1320d-6(b). The maximum fine increases to $250,000 and the maximum term of imprisonment increases to ten years if the offense is "committed with intent to sell, transfer, or use" individually identifiable health information "for commercial advantage, personal gain, or malicious harm." *Id.*

76. Stein, *supra* note 71.

77. *Id.*

78. *Id.*

79. *Id.*

80. *See id.*

81. 42 U.S.C. § 1320d-7(a)(1) (2000); 45 C.F.R. § 160.203 (2007). For instance, the Privacy Rule requires that each covered entity provide its patients a notice of their rights under HIPAA and the Privacy Rule. 45 C.F.R. § 164.520; *see supra* text accompanying notes 64–65. A state law purporting to eliminate this notice requirement would directly contradict the Privacy Rule and would therefore be preempted. *See* 42 U.S.C. § 1320d-7(a)(1); *see also* 45 C.F.R. § 160.203.

patients' privacy interests than the federal rules offer.[82] If state laws protect patients' privacy interests to a greater extent than do HIPAA and the Privacy Rule, there is no federal preemption of the state provisions.[83] In this sense, HIPAA and the Privacy Rule establish a privacy floor for the states; states are free to build upon it but the floor remains.[84] States' exercises of this latitude to provide greater privacy protections have led to a messy legal environment in which differing privacy-preservation obligations exist.[85] As will be seen, the no-preemption rule currently applicable to more protective state-mandated privacy schemes may need to be reconsidered in order to keep privacy concerns, their importance notwithstanding, from becoming an undue barrier to nationwide adoption and clinical interoperability of medical-error-reducing information technology.[86]

Examples of more protective—and hence non-preempted—state privacy rules should be instructive. For instance, in setting the rules concerning HCPs' disclosures of patients' protected medical information, various states' laws are more restrictive[87] than the federal Privacy Rule's provision allowing disclosure without the patient's consent if the disclosure is for purposes of "treatment, payment, or healthcare operations."[88] Where state laws are more restrictive regarding disclosure, they typically require patient consent for some treatment-related disclosures and limit the range of HCPs to whom disclosure may be made without patient consent.[89] Efforts to move toward nationwide use of electronic medical records and related information technology may be impeded by the present requirement that HCPs tailor their operations to comply with some states' differing disclosure rules, as opposed to a single federal standard.[90]

Numerous states' medical privacy laws include significant, though not necessarily identical, restrictions on HCPs' ability to disclose patients' health information insofar

---

82. 42 U.S.C. § 1320d-7(a)–(b); 45 C.F.R. § 160.203. However, if HHS concludes that certain state laws prevent fraud or serve as key components of the state's insurance regulation system, the federal provisions do not preempt the state laws. Neither is there preemption of state laws dealing with controlled substances and with the reporting of injuries, diseases, other public health matters, and vital statistics. 42 U.S.C. § 1320d-7(a)(2), (b); 45 C.F.R. § 160.203. The same is true of state standards and information-gathering efforts that relate to audits, licensure, or certification. 42 U.S.C. § 1320d-7(a)(2), (b); 45 C.F.R. § 160.203.

83. 42 U.S.C. § 1320d-7(a)(2), (b); 45 C.F.R. § 160.203.

84. 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 325, 343 (2002); *see also* Michael D. Greenberg & M. Susan Ridgely, *Patient Identifiers and the National Health Information Network: Debunking a False Front in the Privacy Wars*, 4 J. HEALTH & BIOMEDICAL L. 31, 44–45 (2008); Grace Ko, *Partial Preemption Under the Health Insurance Portability and Accountability Act*, 79 S. CAL. L. REV. 497, 503–04 (2006).

85. Greenberg & Ridgely, *supra* note 84, at 44–45; Ko, *supra* note 84, at 506–10.

86. *See infra* text accompanying notes 90, 95–98, 151–63.

87. *See, e.g.*, FLA. STAT. ANN. § 395.3025 (West 2006); FLA. STAT. ANN. § 465.017 (West 2007); FLA. ADMIN. CODE ANN. r. 64B16-28.130 (2007); GA. CODE ANN. § 24-9-40 (1995); N.H. CODE ADMIN. R. ANN. PH. § 501.01(b)(9) (2005).

88. 45 C.F.R. § 164.506(a); *see supra* text accompanying notes 58–59.

89. *See, e.g.*, FLA. STAT. ANN. § 395.3025; FLA. STAT. ANN. § 465.017; FLA. ADMIN. CODE ANN. r. 64B16-28.130; GA. CODE ANN. § 24-9-40; N.H. CODE ADMIN. R. ANN. PH. § 501.01(b)(9).

90. *See* Hill et al., *supra* note 3, at 231.

as it refers to the patient's having contracted HIV status or other communicable diseases of a serious nature.[91] The federal Privacy Rule, on the other hand, does not treat HIV or communicable disease information differently from other information in terms of healthcare providers' ability to disclose.[92] The state laws are therefore more protective of patient privacy in this respect and would not be preempted by HIPAA and the Privacy Rule.[93] The complying-with-different-standards problem again exists regarding such information and further serves as an example of how the current approach of treating HIPAA and the Privacy Rule as establishing a privacy floor may hinder efforts to develop a national healthcare information network.[94]

This example, however, should not minimize the importance of the patient privacy interests that are at stake. Indeed, the particular sensitivity of such information may make a rule that severely restricts disclosure especially appropriate. But if a special restriction on disclosure of HIV or other communicable diseases information is warranted, adding that special restriction to the federal Privacy Rule—and having one national standard—seems preferable to having a patchwork quilt of state restrictions featuring varying particulars.[95]

Whenever non-preempted state law provisions on medical information privacy differ, they hold the potential for creating confusion and potentially troublesome conflict-of-laws issues. If the patient and her primary care physician are located in a state where her medical record was created, but the primary care physician consults with a specialist in another state, and that specialist in turn consults with an additional specialist in yet another state, which state's law controls in regard to disclosures if the states' laws differ?[96] Instead of HCPs having to worry about such questions and about potential liability for noncompliance with the particular state law deemed controlling,[97] a single nationwide standard sufficiently protective of patients' privacy interests would be more consistent with the realities and needs of modern-day healthcare operations.[98]

---

91. *E.g.*, GA. CODE ANN. § 24-9-47 (1995); IND. CODE § 16-41-8-1 (2008); MO. REV. STAT. § 191.656 (2004); s*ee also* Ko, *supra* note 84, at 506, 523.

92. *See* 45 C.F.R. § 164.506.

93. *See* 42 U.S.C. § 1320d-7(a)(2), (b) (2000); *see also* 45 C.F.R. 160.203.

94. *See* Hill et al., *supra* note 3, at 230–31.

95. *See id.*

96. *See* Greenberg & Ridgely, *supra* note 84, at 45–46.

97. Liability for noncompliance may sometimes be a serious issue under state law, with various states allowing a private right of action to enforce violations of medical privacy restrictions. *E.g.*, R.I. GEN. LAWS § 5-37.3-4 (2004); TENN. CODE ANN. § 68-11-1504 (2006); WASH. REV. CODE ANN. § 70.02.170 (2002); WYO. STAT. ANN. § 35-2-616 (2007); *see also* Pritts, *supra* note 84, at 338. In contrast, there is no private right of action regarding violations of HIPAA and the Privacy Rule. 42 U.S.C. § 1320d-6; 45 C.F.R. § 164.306(a). As noted earlier, the federal government has thus far tended to take a low-key, settlement-oriented approach in handling violations of the Privacy Rule. *See supra* text accompanying notes 69–80. Accordingly, an alleged medical privacy violation that might not lead to adverse consequences for an HCP under federal law or that of most states might trigger patient-instituted litigation in certain states. For reasons of predictability and efficiency, one national rule—either no private right of action or a suitably defined private right—would seem preferable if a national healthcare information network is to become a reality.

98. *See* Hill et al., *supra* note 3, at 213. The multi-state scenario commented on in the text suggests another issue that is not patient privacy-related but stands as an impediment to a

As the foregoing discussion suggests, medical information privacy law has become a federal-state hybrid with troublesome inconsistencies. In the following section, we examine and evaluate previous efforts to harmonize the states' attempts to balance patients' privacy interests against HCPs' need to use and disclose patients' medical information.

III. PAST EFFORTS TO DEAL WITH PRIVACY LAW CONFLICTS

While providing sufficient flexibility to allow system design of effective network architectures, privacy law must concurrently do a reasonable job of protecting patients from privacy invasion.[99] The improper disclosure of health-related information potentially carries more serious consequences than the inadvertent disclosure of many other types of information, as evidenced by the fears of many patients of having their health information compromised[100]—and with good reason.[101] For example, disclosure of an embarrassing disease or disclosure of a mental health illness could unfairly stigmatize an individual.[102] Consequently, privacy laws must be written with patients as a primary concern; but, while strong privacy laws limiting access to this information may comfort patients, care must also be taken to not sacrifice interoperability and information exchange in such a way that treatment is degraded.[103] Effective privacy laws must therefore balance these competing interests.[104]

Substantial efforts have been made toward laying a framework for harmonizing privacy laws. One initiative is the Model State Public Health Privacy Act ("Model Privacy Act") drafted by the Privacy Law Advisory Committee. This model act sets out

---

national healthcare information network: the state-by-state licensing of physicians. Given that HCPs who may need to work cooperatively are these days often located in different states, a scheme of multi-state or national licensing of physicians would likely be superior to the current licensing scheme and the geographic restrictions it places on physicians' ability to practice. *See id.*

99. Vivying S.Y. Cheng & Patrick C.K. Hung, *Health Insurance Portability and Accountability Act (HIPAA) Compliant Access Control Model for Web Services*, 1 INT'L. J. HEALTHCARE INFO. SYS. & INFORMATICS 22, 26 (2006).

100. Andis Robeznieks, *Privacy Fear Factor Arises,* MODERN HEALTHCARE, Nov. 14, 2005, at 6; *see also* Kate Ackley, *Privacy Groups Wary of Health IT Bill*, ROLL CALL, June 19, 2006, at 11.

101. *See, e.g.*, Anne Zieger, *Seattle Health System Will Pay $100K HIPAA Fine*, FIERCEHEALTHIT, July 18, 2008, http://www.fiercehealthcare.com/story/seattle-health-system-will-pay-100k-hipaa-fine/2008-07-18; *WellPoint Data May Have Been Compromised*, FIERCEHEALTHIT, Apr. 21, 2008, http://www.fiercehealthit.com/story/wellpoint-data-may-have-been-compromised/2008-04-21; *U.S. Hospitals Have Security "Blind Spot,"* FIERCEHEALTHIT, Apr. 14, 2008, http://www.fiercehealthit.com/story/u.s.-hospitals-have-security-blind-spot-/2008-04-14.

102. *See* Robert Hanscom, Panel Discussion Remarks, Legal Worries: Clinical Data Sharing, Harvard Medical School Seminar: Patient-Centered Computing and eHealth: State of the Field (Apr. 28-30, 2006) (notes on file with authors) (some patients do not want other providers to see their entire medical histories).

103. *See generally* MODEL STATE PUB. HEALTH PRIVACY ACT (1999), *available at* http://www.publichealthlaw.net/Resources/ResourcesPDFs/modelprivact.pdf.

104. Nancy Vogt, *HIPAA and the Legal Electronic Health Record*, J. HEALTH CARE COMPLIANCE, Nov.–Dec. 2005, at 43, 81; *see Interoperability Clashes with Privacy in Health IT System Development*, WASH. INTERNET DAILY, Jul. 28, 2005 (on file with authors).

ideal standards for protecting PHI.[105] The second initiative, the Turning Point Model State Public Health Act ("Turning Point Act"), borrows heavily from the Model Privacy Act in fashioning a more comprehensive model statute that addresses larger strategic issues in order to help coordinate state-based initiatives for developing public health infrastructure, fostering relationships between the public and private sector, determining the powers of public health agencies, and developing strategies for handling emergencies.[106] The Model Privacy Act and the Turning Point Act might therefore inform legislators and regulators and be guides for privacy protections.

Any model legislation should accomplish the following goals. First, a model law should provide a framework that promotes public confidence in a national healthcare information network.[107] Lack of public trust will undermine the effectiveness of a national healthcare network because some individuals may decide to avoid treatment, research, testing, or other activities that involve the collection of sensitive personal data.[108] Model legislation should inspire confidence in individuals that their most personal information will be reasonably protected from breaches, compromised data, or theft. Additionally, privacy laws should provide the necessary incentives for healthcare organizations to adopt new technologies to improve the quality and efficiency of healthcare.[109]

The two model laws embrace these principles in maintaining that the acquisition of PHI begins with a legitimate public health purpose.[110] In order to acquire PHI, the acquisition should be directly related to this purpose and should be reasonably likely to achieve it.[111] If a healthcare organization can achieve that legitimate purpose with non-identifiable information, then it should defer to that source, only acquiring PHI as a secondary option.[112] Additionally, the model laws would require transparency and

---

105. MODEL STATE PUB. HEALTH PRIVACY ACT, *available at* http://www.publichealthlaw.net/Resources/ResourcesPDFs/modelprivact.pdf.

106. TURNING POINT MODEL STATE PUB. HEALTH ACT, prefatory notes (2003), *available at* http://www.hss.state.ak.us/dph/improving/turningpoint/PDFs/MSPHAweb.pdf.

107. *See generally Activities of the Office of the National Coordinator for Health Information Technology: Hearing Before the S. Subcomm. on Technology, Innovation, and Competitiveness of the S. Comm. on Commerce, Science, and Transportation*, 110th Cong. (2005), *available at* http://www.hhs.gov/asl/testify/t050630a.html (statement of David Brailer, National Coordinator for Health Information Technology); Robert Cunningham, *Action Through Collaboration: A Conversation with David Brailer*, 24 HEALTH AFF. 1150, 1156–57 (2005); Brailer, *supra* note 23.

108. COMM. ON MAINTAINING PRIVACY AND SEC. IN HEALTH CARE APPLICATIONS OF THE NAT'L INFO. INFRASTRUCTURE, NAT'L RESEARCH COUNCIL, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION 2 (1997) [hereinafter FOR THE RECORD]; *see also* Lawrence O. Gostin, James G. Hodge, Jr. & Ronald O. Valdiserri, *Informational Privacy and the Public's Health: The Model State Public Health Privacy Act*, 91 AM. J. PUB. HEALTH, 1388, 1388 (2001).

109. FOR THE RECORD, *supra* note 108, at 2.

110. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-101[a]; MODEL STATE PUB. HEALTH PRIVACY ACT § 2-101[a].

111. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-101[a](1)–(2); MODEL STATE PUB. HEALTH PRIVACY ACT § 2-101[a](1)–(2).

112. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-101[a](3); MODEL STATE PUB. HEALTH PRIVACY ACT § 2-101[a](3).

disclosure. Healthcare organizations cannot surreptitiously acquire PHI,[113] and they must publicly disclose their reasons and intentions for acquiring that information.[114] Finally, the model laws prohibit one public healthcare organization from obtaining data from another unless the acquisition meets the model laws' acquisition standards.[115] Consequently, these laws represent a laudable step in enhancing protection of PHI in various ways. At the same time, however, the restrictions on information transfers between HCPs represent an obvious barrier to large-scale-network system interoperability and information exchange.

In addition to circumscribing when HCPs may acquire PHI, effective privacy laws should define how HCPs use this information after its acquisition. A general principle embodied in the model statutes is that PHI's use should be directly related to the reason for which it was acquired.[116] For example, the model statutes generally allow the use of PHI for research purposes,[117] but prohibit its commercial use.[118] They also define the scope of how health organizations can use the information, and typically restrict the use to the minimum level needed to reasonably accomplish the legitimate purpose.[119] Finally, under the model statutes, organizations must expunge protected information when it is no longer useful in furthering the purpose for which it was acquired.[120]

The foregoing provisions of the model statutes are designed to protect how HCPs acquire and use PHI, but once these organizations have acquired and are using PHI, to whom may it be disclosed? It is this area of disclosure—defining the scope of disclosure and the circumstances permitting disclosure—that promises to be most contentious. Generally, privacy laws recognize that PHI is private and, therefore, prohibit any disclosure unless there is a statutory exception.[121] The most notable exception involves individual consent. Patients may opt to provide their written consent to allow for certain disclosures.[122] Additionally, the model statutes allow for disclosures in emergency situations or to comply with the law.[123] Overwhelmingly,

---

113. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-101[a]; MODEL STATE PUB. HEALTH PRIVACY ACT § 2-101[b].

114. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-101[b]; MODEL STATE PUB. HEALTH PRIVACY ACT § 2-101[c].

115. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-101[c]; MODEL STATE PUB. HEALTH PRIVACY ACT § 2-102.

116. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-102[a]; MODEL STATE PUB. HEALTH PRIVACY ACT § 3-101[a].

117. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-102[f]; MODEL STATE PUB. HEALTH PRIVACY ACT § 3-101[c].

118. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-102[e]; MODEL STATE PUB. HEALTH PRIVACY ACT § 3-103.

119. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-102[c]; MODEL STATE PUB. HEALTH PRIVACY ACT § 3-102[b].

120. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-102[g]; MODEL STATE PUB. HEALTH PRIVACY ACT § 3-104.

121. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-103[a]; MODEL STATE PUB. HEALTH PRIVACY ACT § 4-101.

122. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-103[c]; MODEL STATE PUB. HEALTH PRIVACY ACT §§ 4-101 to -102.

123. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-103[d]–[e]; MODEL STATE PUB. HEALTH PRIVACY ACT §§ 4-104 to -105.

however, the model statutes attempt to limit how organizations share personal information with outside parties, despite the fact that access to a large national database containing data and information about millions of patients would greatly facilitate medical research.[124]

Further, it is not clear that tight restrictions on disclosure, especially restrictions that differ across jurisdictions, always benefit the individual patient because such restrictions could become a barrier to clinical interoperability at a time when the patient desperately needs care.[125] Consider, for example, a situation in which a patient has previously signed a written consent form in her home state to permit disclosure of certain personal health information. Then the patient travels out of state and is injured, necessitating treatment. The out-of-state HCP is required by state law to use only a form approved by that state. Does the patient need to offer his or her consent again due to legal incompatibility?[126] What if the patient is incapacitated at the time? Obviously, as suggested by the model statutes, privacy laws should contain provisions for transfer of patient information in emergencies; however, interstate clinical interoperability would be enhanced by a common, categorical consent instead of requiring point-of-care determination on a case-by-case basis.[127] This raises the question of whether categorical consent should be allowed, or whether legislation should follow the model codes, which generally proscribe it.[128] How should the law handle the balance between protection of patient privacy and the speed of care delivery? Should the desires for privacy by some outweigh the quality of healthcare for others?

Consider further the issue of expunging personal health information that is no longer needed. The provisions in the Turning Point and Model Privacy Acts that require expunging data that no longer furthers the purpose for which it was acquired[129] may be ideal for protecting PHI because privacy is better protected when personal data resides on the fewest possible number of servers.[130] What is uncertain, however, is

---

124. *See, e.g.*, David K. Ahern, Jenifer M. Kreslake & Judith M. Phalen, *What Is e-Health (6):Perspectives on the Evolution of eHealth Research*, J. MED. INTERNET RES., Jan.–Mar. 2006; William T. Lester, Richard W. Grant, G. Octo Barnett & Henry C. Chueh, *Randomized Controlled Trial of an Informatics-Based Intervention to Increase Statin Prescription for Secondary Prevention of Coronary Disease*, 21 J. GEN. INTERNAL MED. 22, 28 (2005); Blackford Middleton, Patricia F. Brennan & Gregory F. Cooper, *Accelerating U.S. EHR Adoption: How to Get There From Here: Recommendations Based on the 2004 ACMI Retreat*, 12 J. AM. MED. INFORMATICS ASS'N 13, 13–15 (2005).

125. John W. Hill & Phillip Powell, *The National Healthcare Crisis:Is eHealth a Key Solution?*, BUS. HORIZONS (forthcoming 2008) (article on file with authors).

126. *See* FOUND. OF RESEARCH & EDUC. OF AM. HEALTH INFO. MGMT. ASS'N, FINAL REPORT PART II: COORDINATING POLICIES THAT IMPACT ACCESS, USE, AND CONTROL OF HEALTH INFORMATION 16–30 (2008), *available at* http://www.slhie.org/Docs/SLHIE_Final_Report_Part11.11.pdf.

127. For discussion of a scenario involving the transfer of medical information in emergency cases, see Hill & Powell, *supra* note 125.

128. *See* TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-103; MODEL STATE PUB. HEALTH PRIVACY ACT § 4-102 cmt. ("General authorization for the release of medical records is insufficient to authorize the disclosure of protected health information.").

129. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-102[g]; MODEL STATE PUB. HEALTH PRIVACY ACT § 3-104.

130. The Model Privacy Act "rejects the view that there is an inherent value to having

under what circumstances privacy laws will permit storage, even temporary storage.[131] Further, who determines when health information is no longer needed? Even though health information is not needed at the moment, who decides that a need may not arise in the future? On a large scale, how will healthcare organizations possessing almost innumerable patient records (containing information that to a significant extent may be idiosyncratic) police outdated information on an efficient basis? It seems likely that expunging initiatives will devolve into arbitrary rules, such as expunging records that have gone for some specified time period without being accessed. Imagine, though, a situation in which an emergency patient is rushed to a healthcare facility five years after her records were last accessed, only to discover that her records have been expunged without her knowledge because of lapsed time. Lawmakers need to recognize that personal health information is dynamic and that privacy laws need to be flexible enough to handle the myriad of unique issues that this information presents as it flows throughout the healthcare system—not only among units of a single healthcare organization, but also among providers, insurers, regulators, and any other entity with access to this information.[132]

There are numerous other questions that arise from the clash of vertically and horizontally incongruous privacy laws. These questions range from seemingly trivial (for example, will cookies be prohibited?) to more serious issues, such as whether software functionality may be degraded by the nonavailability of data that has been expunged by law (as might be the case, for example, when patient baseline data are needed to establish a trend). The model statutes also distinguish between the functions of data acquisition, use, disclosure, and storage,[133] each of which presents its own array of subissues and concerns, many of which are unresolved.[134]

A general principle embodied in the model statutes is that patients should be able to limit who has access to and control of their information, raising questions about authentication—in essence, the assurance that only those individuals who need access to the data are able to access the data.[135] Overly rigid rules for access will inhibit ongoing interoperability. Consider the case of a patient treated for mental illness. Obviously, such information is highly sensitive, and under some conditions it may be unnecessary for a particular treating physician to know that the patient is being treated by another clinician for a mental illness. What if a situation arises, however, in which an emergent physical condition is linked to the mental illness? If the treating physician was previously unaware of the mental illness because of restrictions on access to the

---

identifiable information." MODEL STATE PUB. HEALTH PRIVACY ACT § 3-104 cmt.

131. *Cf.* HEALTH INFO. PROT. TASKFORCE, REPORT FROM HEALTH INFORMATION PROTECTION TASKFORCE TO STATE ALLIANCE FOR E-HEALTH 13–14 (2007), *available at* http://www.nga.org/Files/pdf/0708EHEALTHREPORT.PDF (stating that privacy and security policies should be developed in concert with technology, and one consideration in such an analysis is storage—how does the software store the data and what is the purpose and use of the stored data?).

132. Healthcare information could flow between the doctors and nurses; among the emergency, clinical, or outpatient divisions; or even between the healthcare organization and third parties. FOR THE RECORD, *supra* note 108, at 2–4.

133. *See* MODEL STATE PUB. HEALTH PRIVACY ACT.

134. *See generally id.*

135. Both statutes treat health information as nonpublic information unless the patient consents. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-103[a]–[d] (2003); MODEL STATE PUB. HEALTH PRIVACY ACT § 4-101.

patient's records, how will she become aware? Further, where do the lines of legal responsibility rest for making such need-to-know determinations and informing a treating physician, and who deems a mentally ill patient capable of making such a determination for herself?

As previously stated, clinical interoperability is closely linked to electronic storage and transmission of patient information. This raises the question of whether patients should be compelled to participate in a NHIN.[136] While some maintain that patients should not be forced to participate in an electronic healthcare system because of the perceived risks to patient privacy,[137] others maintain that patients who opt out of such a system would raise the costs for all, as well as the risks for themselves.[138] It remains to be seen how this knotty issue will be resolved.

The foregoing discussion suggests four points. First, although there is evidence that the model statutes have influenced some state legislatures, lawmakers should be informed by them in forging future laws.[139] This will engender the systemic transparency necessary to inspire adequate patient confidence in the network and thereby encourage use of any NHIN. That is, individuals should understand the circumstances and the scope of how the health organizations will acquire, use, disclose, and store their personal information. Given the highly diverse nature of healthcare services consumers—representing all ages, levels of educational attainment, and socioeconomic backgrounds—it seems Pollyannaish to believe that such understanding will be universal.

Second, the model privacy laws seemingly understand the nature of healthcare information well. Privacy laws should consider how entities acquire and use data so that data acquisition and use are reasonably tethered to the stated purpose for acquiring the information.[140] Once the information is acquired, organizations should take steps to ensure that it is not irresponsibly disclosed and is protected from security threats.[141] The model statutes appear to be more accommodative of some of the nuances inherent in PHI (for example, protecting against disclosure of HIV or other communicable diseases) than HIPAA. In some ways, these models represent general ideals for protecting privacy and are an important step toward reducing conflicts among the patchwork of federal and state privacy laws that impede the information exchange critical to clinical interoperability.[142] Lawmakers need to go beyond general ideals and recognize that effective privacy laws are dependent not only on legal reform, but also

---

136. *See Electronic Health Records and the National Health Information Network: Patient Choice, Privacy, and Security in Digitized Environments Before the Subcomm. on Privacy and Confidentiality of the National Comm. on Vital and Health Statistics* (2005) (statement of Pam Dixon, Executive Director, World Privacy Forum), *available at* http://www.worldprivacyforum.org/testimony/CVHStestimony_092005.html.

137. *See* Gostin et al., *supra* note 108, at 1388–90.

138. *See, e.g.*, Hill et al., *supra* note 3, at 233 & n.525.

139. *See generally* TURNING POINT, TRANSFORMING PUBLIC HEALTH STATE BY STATE, *available at* http://www.turningpointprogram.org/toolkit/pdf/TP_state_booklet.pdf (summarizing the various state programs).

140. *See* Hill et al., *supra* note 3, at 188–93 (discussing the implementation of the HIPAA and the Privacy Rule promulgated by HHS).

141. *See id.*

142. *See, e.g.*, Camin, *supra* note 39.

on support activities—such as training, improved infrastructure for privacy surveillance, and health privacy education—that should supplement legal reform.[143]

Third, the model laws seemingly do not resolve information exchange conflicts at the clinical level particularly well; nor do they create real incentives to dismantle interstate barriers that have been erected by state legislatures passing disparate privacy laws that are more restrictive than either those contemplated in the HIPAA Privacy Rule or the model statutes. As noted in previous sections, many inconsistencies and unanswered questions remain regarding clinical interoperability and health information availability, access, and exchange. The model laws, then, appear to represent only a set of general ideals and are neither a detailed implementation guide nor a mandate for harmonization.

Finally, privacy laws must delicately balance the competing concerns of privacy and interoperability.[144] Although there is nothing new about this observation, it is perhaps noteworthy that a balance requires a fulcrum. The problem of achieving the appropriate balance is therefore complicated by the dynamic nature of healthcare consumerism, which makes the fulcrum nonstationary as healthcare moves from being patient-centric to consumer-centric and patients' risk tolerance with respect to healthcare information changes. On the one hand, consumerist patients will almost certainly demand that more information about their health be retained by healthcare institutions, thereby increasing the risk of compromising private information and suggesting tighter restrictions on its availability.[145] On the other hand, as consumerist patients become more educated and involved in their healthcare they are also more likely to demand higher-quality healthcare.[146] This leads inexorably back to the need for greater clinical interoperability and, concomitantly, more information exchange. This is yet another contrarian paradox in healthcare that raises the stakes on both sides of the cost-benefit equation. If a state legislature enacts a tough privacy law, then interoperability becomes an issue;[147] but, if the privacy law is not protective enough, then individual privacy is more likely to be compromised.[148] The problem, therefore, remains a difficult one for which there is likely no Pareto optimal solution[149] that will satisfy everyone.

IV. WHAT CONCLUSIONS CAN WE DRAW?

In the end, the solution of deconflicting federal and state privacy laws will logically follow one of three paths. One solution is a bottom-up approach in which all states voluntarily and multilaterally harmonize their healthcare privacy rules around some set

---

143. Lawrence O. Gostin & James G. Hodge, Jr., *The Public Health Improvement Process in Alaska: Toward a Model Public Health Law*, 17 ALASKA L. REV. 77, 114 (2000).

144. Hill et al., *supra* note 3, at 226–30.

145. DELOITTE CTR. FOR HEALTH SOLUTIONS, *supra* note 35, at 22.

146. *Id.*

147. *See* Gostin & Hodge, *supra* note 143, at 115.

148. *See id.*

149. JOEL S. DEMSKI, INFORMATION ANALYSIS 84–85 (2d ed. 1980) ("[A] group utility assessment across two alternatives must be such that if each individual strictly prefers the first to the second alternative, then the group assessment must strictly prefer the first to the second. This condition is termed *Pareto optimality*.") (emphasis in original).

of common objectives and federal law. This seems unlikely to happen in any reasonable timeframe given the absence of a group utility function.[150] Alternatively, the federal government could impose top-down legislation preempting state law altogether. Given that this path would likely be fraught with political difficulties, a third approach involving some attempt to combine federal and state law in line with Congress's prior intent may prove tempting. This latter approach might retain the notion of a federal privacy law floor by both broadening and deconflicting HIPAA and then inviting states to layer laws upon it. Although perhaps at first blush this approach seems more appealing than either multilateral harmonization or complete federal preemption, it has problems as well.

A major problem with harmonizing federal and state law is the narrow scope of HIPAA Privacy Rule coverage.[151] For example, HIPAA's definition of a "covered entity" includes health plans, healthcare clearinghouses, and HCPs who transmit any health information in electronic form in a standard transaction.[152] Left out of this definition are organizations such as employers, insurance companies other than health insurers, and others who may encounter patient health information in the normal course of their activities. An expansion of this definition to include *all* parties in possession of patient health information would help reduce inadvertent compromises.[153] If states were left to their own volition, however, there would be no assurance that they would create uniform definitions of covered entities.

This concern may lead to the temptation to link HIPAA and a set of federal statutes, as contemplated in the Turning Point Act with its emphasis on patient consent as a prerequisite for disclosure.[154] In this marriage, model statutes might be designed to work in tandem with the HIPAA Privacy Rule, filling voids such as the under-inclusive definition of "covered entity" discussed in the previous paragraph. Other voids might remain the responsibility of state legislatures, with the hope that model statutes would drive the scope and nature of state law. The prospects for such a compromise solution do not appear sanguine, however, inasmuch as federal and state authorities appear to disagree with the layered approach, with some holding that HIPAA preempts state law and others concluding that it does not.[155]

---

150. *Id.* ("The difficulty . . . is that *no* group utility assessment exists that will satisfy these relatively innocuous requirements . . . . Requiring even modest standards of assessment, the fancied group measure does not exist.") (emphasis in original).

151. *See* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 360 (2007).

152. 45 C.F.R. § 160.103(3) (2007).

153. Hoffman & Podgurski, *supra* note 151, at 360.

154. TURNING POINT MODEL STATE PUB. HEALTH ACT § 7-101[a] (2003).

155. The Turning Point Act is supposed to work in harmony with HIPAA, but commentary suggests that the disagreement between the state and federal authorities as to whether HIPAA preempts state law makes a compromise solution less likely. *See* U.S. Dep't Health & Human Servs., How Does the HIPAA Privacy Rule Reduce the Potential for Conflict with State Laws?, http://www.hhs.gov/hipaafaq/state/401.html; TURNING POINT MODEL STATE PUB. HEALTH ACT art. VII prefatory notes.

Moreover, the danger of a federal and state law shotgun marriage becomes apparent when one considers the HIPAA Privacy Rule's evolution.[156] After Congress passed HIPAA, it directed HHS to submit recommendations for uniform national privacy standards to Congress.[157] When Congress failed to enact further legislation promulgating final privacy standards, the responsibility fell to the Secretary of Health and Human Services to fill the gap.[158] What resulted was the Privacy Rule, a set of privacy regulations designed to establish a federal floor for privacy regulation such that HIPPA does not preempt the state law as long as it imposes more stringent requirements, standards, or implementation specifications with respect to individually identifiable health information.[159] If, however, Congress failed to act due to political disagreement, what assurance is there that state legislatures will not emulate Congress?

Additionally, despite the intent that federal law be a floor upon which to build, marrying federal and state laws has not turned out to be a smooth process. The HIPAA Privacy Rule and HIPAA preemption analysis have added complexity to the resolution of conflicts between federal and state law in some cases. Although Congress and HHS intended the HIPAA Privacy Rule to be a floor for healthcare privacy law, it has become more than just a floor; and its occasional conflicts with state law, if left unresolved, could leave network architects with no choice but to use HIPAA as the sole industry standard, despite its shortcomings.[160]

These considerations cast serious doubt upon the efficacy of integrating existing laws, a doubt that is consistent with the position of at least one expert who believes that it would be a mistake to "try and shoehorn the NHIN into the [P]rivacy [R]ule framework."[161] The salient question, then, boils down to the following: can states be expected to voluntarily and almost simultaneously remove these privacy law barriers bottom-up by agreeing to harmonize through compromise, or is a top-down solution necessary?[162] Given the ponderous pace at which healthcare reform has proceeded in the past when relying primarily on bottom-up approaches,[163] it seems unlikely that adequate incentives currently exist for a bottom-up approach to work well, despite the national crisis. This seems especially true in light of the absence of any Pareto optimal solution for balancing health information access against strict privacy safeguards. By process of elimination, then, a top-down approach is seemingly the only way to remove

---

156. 42 U.S.C. §§ 1320d-1 to -8 (2000); 45 C.F.R. §§ 160.103–160.104, 164.502–160.503 (2007).

157. 42 U.S.C. §§ 1320d-1 to -3.

158. *See id.*; 45 C.F.R. §§ 160.103–160.104, 164.502–160.503.

159. 42 U.S.C. § 1320d-7(a)(2); 45 C.F.R. § 160.203; *see also supra* text accompanying notes 81–86.

160. Sean T. McLaughlin, *Pandora's Box: Can HIPAA Still Protect Patient Privacy Under a National Health Care Information Network?*, 42 GONZ. L. REV. 29, 53–55 (2006).

161. *NCVHS Privacy Chair Sees NHIN as 'A Chance to Rethink Everything' in Privacy Regulation*, REP. ON PATIENT PRIVACY, July 1, 2006 (quoting Mark Rothstein, Privacy Subcommittee Chairman of the National Committee on Vital and Health Statistics, which provides guidance to the Department of Health and Human Services).

162. *See id.*

163. *See, e.g.*, Paul Starr, *What Happened to Healthcare Reform?*, THE AM. PROSPECT, Fall 1994, at 20, 20–31.

the privacy law barriers delaying rapid healthcare reform.[164] If a top-down approach is needed, what latitude, if any, should be left for state law layering purposes when any such latitude runs some risk that state law will interfere with interstate clinical interoperability and health information exchange?

The bad news is that during the recent presidential campaign, it was not apparent that either of the presidential candidates—whose concerns appeared to be narrowly focused on short-term accessibility and affordability issues rather than more holistic approaches to dealing with the healthcare crisis—appeared to grasp the full set of problems the nation faces in achieving a high-quality healthcare system that is both affordable and accessible by the vast majority of the populace.[165] Consequently, the presidential campaign rhetoric about healthcare reform may not be a precursor to sweeping reform of privacy laws. Yet sweeping reform may be the only reasonably expeditious path to remove this barrier to interstate clinical interoperability and information exchange.

The good news is that it appears Washington is gearing up for what promises to be another major healthcare reform effort; and, unlike the 1994 attempt, "the stars may be aligned for Congress to make big changes."[166] Should Congress and the next Administration decide to enact sweeping patient privacy legislation, the most viable approach would appear to be filling the voids in existing federal laws and providing financial incentives for state compliance that are of such magnitude that noncompliance becomes economically unpalatable. In this vein, an analogy might be drawn to federal highway funding, the receipt of which depends upon conformity to a set of federal standards.[167]

The stakes involved with healthcare reform are very high. As two distinguished commentators, Julius Richmond and Rashi Fein, have stated, "[t]here is a disconcertingly large gap, more correctly a chasm, between the scientific glories of American medicine and the delivery failures of the American health care system."[168] Moreover, "today's health care system, the manner in which it is organized, its level of funding, and the ways that health services are financed for and by our population are not meeting our nation's requirements."[169] Finally, Richmond and Fein state that: "On the one hand we are the only [first-world] country without universal entitlement to health care services and thus have a large number of uninsured. On the other, we spend far more on health care, both per capita and as a percentage of GDP, than any other country."[170]

---

164. After all, "'[g]erms and patients don't really recognize state boundaries.'" Heather B. Hayes, *Doctors with Borders*, GOV'T HEALTH IT, Nov. 5, 2007, at 36–37 (quoting Robert Steffel, CEO of Healthbridge), *available at* http://www.govhealthit.com/print/4_13/rhio_report/350081-1.html.

165. Brailer, *supra* note 23.

166. Lori Montgomery, *Writing New Prescriptions for Change*, WASH. POST, June 17, 2008, at D1.

167. *See* 23 U.S.C. § 109 (2006).

168. RICHMOND & FEIN, *supra* note 13, at 1.

169. *Id.* at 191.

170. *Id.* at 232.

We can only hope that, following the recent presidential election, politicians will put aside partisanship, strive for a more complete grasp of the healthcare crisis, and begin to deal meaningfully and holistically with the healthcare challenges facing the nation—including those emanating from complicated and conflicting privacy laws.