THERE IS A TIME TO KEEP SILENT AND A TIME TO SPEAK, THE HARD PART IS KNOWING WHICH IS WHICH: STRIKING THE BALANCE BETWEEN PRIVACY PROTECTION AND THE FLOW OF HEALTH CARE INFORMATION

Daniel J. Gilman[*]
James C. Cooper[**]

Cite as: Daniel J. Gilman and James C. Cooper, *There Is a Time to Keep Silent and a Time to Speak, the Hard Part Is Knowing Which Is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. TECH. L. REV. 279 (2010), *available at* http://www.mttlr.org/volsixteen/gilman&cooper.pdf

* Daniel J. Gilman, J.D., Ph.D., is an Attorney-Advisor in the Office of Policy Planning at the Federal Trade Commission.

** James C. Cooper, J.D., Ph.D., is Attorney-Advisor to Commissioner William E. Kovacic at the Federal Trade Commission. The views expressed in this Article are those of the authors alone, and do not necessarily represent the views of the Federal Trade Commission or any of its commissioners. The authors would like to thank Maureen K. Ohlhausen, William E. Kovacic, and Arlene Holen for their helpful comments regarding earlier drafts of this Article and related materials. Faults in this Article should, of course, be attributed to the authors alone.

Every positive value has its price in negative terms.
—Pablo Picasso

INTRODUCTION

Here comes a transformation, again. Health information technology (HIT) has become a signal element of federal health policy, especially as the recently enacted American Recovery and Reinvestment Act of 2009 (Recovery Act or ARRA)[1] comprises numerous provisions related to HIT and commits tens of billions of dollars to its development and adoption.[2] These provisions charge various agencies of the federal government with both general and specific HIT–related implementation tasks including, *inter alia*, providing funding for HIT in various contexts: the implementation of interoperable HIT, HIT–related infrastructure, and HIT–related training and research. The Recovery Act also contains various regulatory provisions pertaining to HIT. Provisions of the Recovery Act that address HIT directly require the establishment of the Office of the National Coordinator for Health Information Technology (ONCHIT or ONC) at the Department of Health and Human Services (HHS)[3] and specify incentive payments for health care professionals and hospitals to implement, improve, and maintain HIT under the Medicare and Medicaid programs.[4]

1. The "American Recovery and Reinvestment Act of 2009" is the short title of H.R.1, "Making supplemental appropriations for job preservation and creation, infrastructure investment, energy efficiency and science, assistance to the unemployed, and State and local fiscal stabilization, for fiscal year ending September 30, 2009, and for other purposes." American Recovery and Reinvestment Act of 2009 (Recovery Act), Pub. L. No. 111-5, 123 Stat. 115 (2009).

2. Although $19, $20, and $22 billion price tags have been associated with Recovery Act HIT spending, HIT-related outlays contemplated in the statute appear to be much higher still. A partial tally may be gleaned from notes 3–4, *infra*. *See generally* Letter from Douglas W. Elmendorf, Dir., Cong. Budget Office, to Hon. Charles E. Grassley, Ranking Member, Comm. on Fin., U.S. S., tbl.2 (Mar. 2, 2009), http://www.cbo.gov/ftpdocs/100xx/doc10008/03-02-Macro_Effects_of_ARRA.pdf.

3. *See* Recovery Act § 3001. The Congressional Budget Office (CBO) has estimated budget authority of $2 billion and outlays of $1.98 billion associated with Title XIII. Letter from Douglas W. Elmendorf, *supra* note 2, at tbl.2.

4. For these provisions in Division B, Title IV, of the Recovery Act, CBO estimates net outlays at $20.819 billion. Letter from Douglas W. Elmendorf, *supra* note 2, at tbl.2. That estimate supposes substantial savings in later years. For example, CBO-estimated total outlays for Medicare incentives total $36.347 billion from 2009 through 2015, but anticipated negative

Although the magnitude of this commitment to HIT is striking, the impetus is clear enough.[5] Many have argued that the growth of HIT is critical to improving quality and efficiency in health care delivery.[6] It appears that HIT has the potential to reduce medical errors,[7] duplicative testing and procedures,[8] and substantial administrative costs now attributed to incomplete, hard–to–find, or otherwise faulty paper records.[9] Although significant use of computers in health care dates to at least the 1950s, many areas of health care trail other sectors of the economy in their use of information technology. How is it that in many practices, the use of expensive and highly sophisticated technology—such as magnetic resonance imaging—is common, but the use of simple technology—such as computerized lookup tables to check both general and patient–specific contraindications for prescription medicines—is not?

The answer is not so simple. On the one hand, certain barriers to widespread adoption of HIT have been plain enough and are well documented. As described below, the costs of adoption, which are borne chiefly by health care providers, can be high, including not only the acquisition of hardware and software but often costs associated with modifying HIT systems to suit particular practices, training for users, and prospective maintenance and updating costs.[10] At the same time, the

outlays (savings) total $15.528 billion from 2016 through 2019. HHS has estimated spending "$44.7 billion in incentives through Medicare and Medicaid to encourage physicians and hospitals to adopt certified electronic health record (EHR) technology." Dep't of Health & Human Servs., Fiscal Year 2010 Budget in Brief: American Recovery and Reinvestment Act, http://www.hhs.gov/asrt/ob/docbudget/2010budgetinbriefc.html (last visited Mar. 24, 2010). Outlays may run to $50 billion, as they represent mandatory spending in payments due to all physicians and hospitals complying with the required criteria. *See* Tevi Troy, *5 Myths on Health Care's Electronic Fix-It*, WASH. POST, Apr. 26, 2009, at B3. Smaller allocations to HIT-related programs are made elsewhere in the Act, while other provisions provide for the funding of various programs that include, but are not limited to, HIT.

5. Certainly, many private and public initiatives precede this one. Indeed, the ONC itself was initially established not under the Recovery Act's statutory mandate, but under a 2004 executive order. *See* Exec. Order No. 13,335, 69 Fed. Reg. 24,059 (Apr. 30, 2004) [hereinafter 2004 Exec. Order].

6. *See* Richard Hillestad et al., *Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs*, 24 HEALTH AFF. 1103, 1103 (2005).

7. *See* BD. ON HEALTH CARE SERVS., INST. OF MED., PREVENTING MEDICATION ERRORS 5 (Philip Aspden et al. eds., 2006) (estimating a minimum of 1.5 million preventable medication errors per year in hospitals, nursing homes, and ambulatory care settings in the United States). The IOM has also identified HIT as a promising means of reducing the frequency of such errors. *See id.* at 6, 223–36.

8. *See id.* at 13–14 (discussing the importance of electronic prescribing and other HIT in reducing medication errors).

9. *See id.* at 6, 13–14, 223–36.

10. *See* CONG. BUDGET OFFICE, EVIDENCE ON THE COSTS AND BENEFITS OF HEALTH INFORMATION TECHNOLOGY 17–18 (May 2008), *available at* http://www.cbo.gov/ftpdocs/

benefits of adoption tend to be distributed, accruing mostly to payers, patients, and public health rather than to the health care providers who pay the direct costs of adoption. The Recovery Act promises to shift that balance of costs and benefits in a way that is bound to be significant. Specifically, the Act's financial incentives for adoption should make at least a marginal difference for many practitioners, practices, and hospitals.

The problem of adoption has not, however, been a simple problem of misaligned incentives, and it is unlikely that the allocation or re–allocation of funds will remove all of the barriers to the widespread adoption of fully functioning, interconnected, HIT systems by U.S. health care providers. First, despite the considerable promise of HIT, implementation can be difficult, and deliverable off–the–shelf benefits are unclear to many providers, independent of price and payment questions. Other significant impediments to HIT adoption include complex "cultural" barriers among practitioners and patients, standard–setting issues, network externalities, and regulatory costs. These are surveyed briefly below, both because some general background is useful to our particular discussion and because these impediments are, in various ways, interrelated. Our focus in this Article, however, will be on one particular species of regulatory costs—those imposed by certain sorts of privacy and data security regulations, with special attention to state law privacy and data security regimes.

There are several reasons for this focus. First, lowering these sorts of barriers may sometimes be tractable and cost–effective. Regulatory reform is not always low–hanging fruit, but it may be more practicable in the short run than, say, reworking the medical practice habits of several generations of established, working physicians. Second, emerging research casts new light on the relationship between privacy regulation and HIT in ways important to HIT policy. Recently, several authors have provided cogent analyses of the implications of HIT for health information privacy, and have suggested regulatory modifications to ensure that privacy remains protected.[11] In addition, emerging research suggests that, by increasing the costs of inter–hospital communication of health information, certain state privacy laws tend to suppress the network benefits associated with HIT, and thus tend to reduce the rate of HIT adoption by

91xx/doc9168/05-20-HealthIT.pdf?bcsi_scan_DA3493EE5FC9D524=0&bcsi_scan_filename=\05-20-HealthIT.pdf.

11. *See*, *e.g.*, Sharona Hoffman & Andy Podgurski, *Electronic Health Record Systems*, 22 HARV. J.L. & TECH. 104, 121–22 (2008); Sharona Hoffman & Andy Podgurski, *Protecting Electronic Private Health Information*, 48 B.C. L. REV. 331, 335–38 (2007); Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 682.

hospitals in those states that have such laws.[12] That result may not be wholly surprising, as many stakeholders have suggested that certain state laws may impede HIT adoption,[13] and that the mix, or patchwork, of state regulation is problematic as it stands.[14] Third, building on both these strands of research, we will argue that policy makers should consider tradeoffs between two important policy goals that are to some extent in tension: (1) regulatory protections for health information privacy and (2) the flow of health information, which is a central goal of HIT. The Recovery Act does not seem to recognize such tradeoffs, although we hope that they may figure in its implementation.

At one level, tradeoffs between privacy and HIT are inevitable. HIT facilitates the collection, storage, processing, and flow of health information. Privacy and data security depend, at least, on the absence of unwanted access to or sharing of health information. Hence, many of the benefits associated with HIT arise from rapid and low–cost information sharing between disparate parts of the health care system, but laws designed to protect health privacy are designed to make the flow of health care information more costly. Indeed many states have been working to update and harmonize their regulatory requirements in this area in recognition of such problems.[15] In this Article, we examine the balance between patients' legitimate concerns about the breach of health information privacy and security, on the one hand, and the HIT–associated benefits that may be threatened by excessive and highly variable privacy regulation, on the other. As has been argued in the context of financial privacy,[16] we contend that HIT privacy policy should be guided by the

12. *See, e.g.*, Amalia R. Miller & Catherine Tucker, *Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records* 55 MGMT. SCI. 1077 (2009) (discussing the differential effects of state law medical privacy regimes on hospitals' adoption of HIT).

13. *See, e.g.*, LINDA L. DIMITROPOULOS, PRIVACY AND SECURITY SOLUTIONS FOR INTEROPERABLE HEALTH INFORMATION EXCHANGE: NATIONWIDE SUMMARY 6-3 (2007) [hereinafter NATIONWIDE SUMM.] ("Several states reported that antiquated laws written for paper-only environments created significant barriers to electronic health information exchange.") .

14. *See, e.g.*, Linda Dimitropoulos & Stephanie Rizk, *A State-Based Approach to Privacy and Security for Interoperable Health Information Exchange*, 28 HEALTH AFF. 428, 428–29 (2009) ("An interoperable system of HIE [health information exchange]—that is, one in which various parties can share and exchange data among them—will have difficulty accommodating the current range of variation in policy requirements."); *see also, e.g.*, J. Thomas Rosch, Comm'r, F.T.C., Where Do We Go From Here?—Some Thoughts on the Future of the Consumer Protection Mission (Jan. 29, 2007) (transcript available at http://www.ftc.gov/speeches/rosch/070129RoschABAconsprotconf.pdf).

15. *See, e.g.*, NATIONWIDE SUMM., *supra* note 13, at 6-39 to 6-44 (reporting on various cross-state and interstate initiatives to address interstate variation, including efforts to harmonize state medical privacy laws across certain states).

16. *See* J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 118–20 (2008).

expected consequences of breach—both tangible harms and the impact on the intrinsic value that patients find in health information privacy. Data suggest that the former harms are small, and we suggest that policy makers should develop a keener understanding of the latter, which is likely to vary across the population in both quality and magnitude.

We investigate the expected tangible privacy harms related to HIT and find them to be less stark than some may believe. For example, from 2001 to 2005, about 0.111% of the adult population suffered medical insurance account misuse (defined as the use of personal information to obtain or receive payment for medical treatment, services or goods), and only 0.0148% of the adult population had their personal data used to create a new medical insurance policy.[17] Further, it does not appear that consent or breach–notification requirements significantly reduce the tangible harms caused by the privacy violations that do occur. Rather, most benefits from medical privacy regulations likely accrue in the utility that patients derive from the fact that they have dominion over their personal medical information. This likelihood strongly suggests that policy makers need to develop a clearer understanding of patients' underlying preferences for medical privacy *before* expanding regulatory burdens, as they ought to be wary of adopting costly regulations that may promise modest tangible benefits. In light of the existing data on consumer preferences for privacy, we propose a modified federal Privacy Rule that maintains the exception to consent for medical treatment, but also allows privacy–sensitive patients to sequester their records from interoperable HIT systems altogether. We also suggest that breach notification triggers should be related to actual risk of harm and that a focus on data security may be a more efficient substitute for both consent and breach notification requirements.

We also focus on the costs associated with varying state regulation of medical privacy. Although we do not advocate any particular legislative response to the costs of state regulation, we explain how the express preemption of state health information privacy and data security provisions could be an efficient response to the costs of those provisions. In addition, although the implied preemption arguments advanced by the petitioners (and rejected by the U.S. Supreme Court) in another health

17. *See* SYNOVATE, 2006 IDENTITY THEFT SURVEY REPORT 17, 19 (2007), http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf [hereinafter SYNOVATE 2006 REPORT]. These calculations are based on an estimate of 3.7% of the adult population being a victim of ID theft. *Id.* at 11. Of the surveyed victims of ID theft, 3% suffered reported misuse of existing medical insurance accounts. *Id.* at 17. Also, 0.04% of surveyed ID theft victims reported that new medical insurance accounts were opened using the stolen information. *Id.* at 19. Thus, .03 * .037 = 0.00111 of the adult population suffered misuse of their existing medical insurance accounts and .004 * .037 = 0.000148 of the adult population suffered new medical insurance account fraud.

care context, that of *Wyeth v. Levine*,[18] are precluded by statute in this one,[19] policy arguments in favor of preemption in this area may enjoy certain advantages that, at least in the Court's view, were not available to the petitioners in *Wyeth*.

Nothing in the following discussion should be read to assail the notion that some form of regulatory intervention is appropriate to safeguard the substantial consumer interests at stake in the area of health information privacy.[20] But excessive regulation, or a poorly integrated patchwork of federal and state regulations, could impede innovations that would be beneficial to health care consumers, public health, and the fisc.[21] Even well–intentioned regulations can be costly, and the research community only recently has begun to grapple with the broader costs—including the economic and health costs—of various means of safeguarding consumer privacy. Because substantial attention rightly is being paid to the consumer interests at stake in HIT privacy and data security, we focus here on the other side of the cost/benefit divide.

This Article is unique because, in addition to its use of independent research, it draws heavily from information gathered at a 2008 Federal Trade Commission workshop that examined certain innovations in health care delivery (the Workshop).[22] The Article proceeds as follows. Part II comprises several brief background sections: (a) summarizes certain general information about HIT development and adoption; (b) reviews certain costs and benefits associated with HIT; and (c) provides an overview of federal and state health information privacy and data security law. Part III returns to the question of benefits and barriers associated

18. Wyeth v. Levine, 129 S. Ct. 1187, 1193–94 (2009).

19. Regulations promulgated under HIPAA with regard to "the privacy of individually identifiable health information shall not supercede 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." Health Insurance Portability and Accountability Act of 1996 (HIPAA) § 264(c)(2), 110 Stat. 2033–34, 42 U.S.C. § 1320d-2 (2009).

20. *See, e.g.*, United States v. Skodnek, 933 F. Supp. 1108 (D. Mass. 1996) (describing harms to consumers related to defendant psychiatrist who was fined and incarcerated following convictions for making false claims to the Medicare program, mail fraud, obstruction of justice, and witness intimidation); *cf.* ALAN F. WESTIN, HOW THE PUBLIC VIEWS PRIVACY AND HEALTH RESEARCH 13–14 (2008), *available at* http://www.ftc.gov/os/comments/healthcarewrkshp/534908-00001.pdf (suggesting through nationwide survey data that 58% of respondents believe medical-record privacy is insufficiently protected).

21. *See* Amalia Miller, Professor, Dep't of Econ., Univ. of Va., Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 225–32, 251–52 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf).

22. The main web page for the April 24, 2008 FTC Workshop, Innovations in Health Care Delivery, with links to the Workshop agenda, a complete transcript of the Workshop itself, supporting materials, and public comments, is available at http://www.ftc.gov/bc/healthcare/hcd/index.shtm.

with HIT, providing a more focused discussion of network effects in HIT. Part IV examines consumers' demand for privacy generally and health information privacy specifically. Part V then analyzes the implicit tradeoffs between various types of privacy regulation and the adoption and application of HIT. Part VI considers the federal preemption of state regulation of health information privacy and data security as a feasible policy response to the costs of regulatory variation.

I. TECHNICAL, MARKET, AND REGULATORY BACKGROUND

A. *The Development and Adoption of HIT*

As noted above, many areas of health care trail other sectors of the economy in their use of information technology. Recent years, however, have seen a proliferation of utilities, systems, hardware, and analytics, including electronic health records, personal health records, electronic prescribing, and the collection, analysis, and flow of increasingly rich types of health information. Generally speaking, HIT "refers to computer applications for the practice of medicine."[23] "Applications," in this context, encompass software and hardware applications and their outputs, as well as analytic, training, and other support services that might enhance the use of such applications.

The Recovery Act stipulates that " 'health information technology' means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information."[24] Just as the Recovery Act thus defines HIT generally for certain of its own purposes, it is important to understand that HIT comprises myriad products and services, such as (a) electronic medical records—including patient records, clinical decision support, laboratory records, health plan records, records exchange systems, and personal health records, (b) clinical ancillaries and other kinds of clinical information systems, such as labs, radiology, and image management systems, (c) biomedical devices, including medical device data systems, (d) population HIT, including "not just public health reporting, which is moving to an electronic basis, but also registries such as disease registries, immunization registries, and . . . statistical analysis and reporting such as quality of process, quality of outcomes and health disparities

23. CONG. BUDGET OFFICE, *supra* note 10, at 1.

24. American Recovery and Reinvestment Act of 2009 (Recovery Act), § 3000(5), 123 Stat. 115, 229 (2009).

analysis that would count in the population health area of health IT," and (e) applications serving the administrative and financial sectors of medicine.[25]

Note, too, that there appears to be substantial variation in usage in broader discussions of HIT,[26] and that definitions may continue to change in the course of HIT development. As a practical matter, this Article makes no attempt to force the larger HIT policy discussion—including published research—to conform to particular stipulated definitions of HIT applications. At the same time, certain extant definitions of central HIT applications provide a useful baseline. In 2008, the National Alliance for Health Information Technology offered the following definitions in a report to the ONC:

- Electronic Medical Record [eMR]: An electronic record of health–related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization.
- Electronic Health Record [eHR]: An electronic record of health–related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization.
- Personal Health Record [PHR]: An electronic record of health–related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.[27]

25. At the FTC Workshop, Mr. Ferguson provided roughly this overview of HIT applications, devices, and services. James Ferguson, Exec. Dir., Health I.T. Strategy & Policy, Kaiser Permanente, Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 135–36 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf).

26. *See, e.g.*, OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., PERSONAL HEALTH RECORDS AND THE HIPAA PRIVACY RULE 1, http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf (last visited Mar. 24, 2010) ("There is currently no universal definition of a [Personal Health Record], although several relatively similar definitions exist within the industry.")

27. NAT'L ALLIANCE FOR HEALTH INFO. TECH., DEFINING KEY HEALTH INFORMATION TECHNOLOGY TERMS 6 (2008), http://healthit.hhs.gov/ (use the search bar to locate the document and then follow the hyperlink).

For the most part, the Recovery Act appears to have borrowed from these in its stipulated HIT definitions.[28] Also important is electronic prescribing (eRx), which has been "defined by the eHealth Initiative as 'the use of computing devices to enter, modify, review, and output or communicate drug prescriptions.' "[29]

Again, many have argued that the growth of HIT is centrally important to improving quality and efficiency in health care.[30] Both the general promise of HIT and its demonstrated efficiencies in particular implementations have garnered substantial private and public commitment to HIT development and adoption. Large IT businesses are increasingly involved in HIT development;[31] large employers have been interested in the potential benefits of HIT for their health care benefits programs;[32] and prior to the Recovery Act's enactment, HHS and other federal agen-

28. For example, under the Recovery Act, an "electronic health record" (eHR) is "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff." Recovery Act § 13400(5).

29. Agency for Healthcare Research and Quality, Electronic Prescribing, http://healthit.ahrq.gov/ (follow the "Electronic Prescribing" hyperlink in the "Key Topics" box) (last visited Mar. 24, 2010). We stipulate the use of "eRx" as a convenient abbreviation for electronic prescribing for the purposes of this Article.

30. *See, e.g.*, Hillestad et al., *supra* note 6, at 1103.

31. For example, the Workshop included a presentation on Microsoft's Health Vault, a platform supporting web-based PHRs and the development of various HIT applications that might interconnect with such PHRs. George Scriban, Senior Product Manager, HealthVault, Microsoft, Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 235–48 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf). Discussion also included the third-party PHR application Google Health, which, like Health Vault, provides individual health care consumers with web-based tools with which to populate their records. *See* Deven McGraw, Dir., Health Privacy Project, Ctr. of Democracy and Tech., Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 145 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf); *see also* Google Health, http://www.google.com/health (last visited June 6, 2008). At the same time, part of what is striking about HIT development is the extent to which health care providers themselves have found it necessary to develop such proprietary HIT systems. At the Workshop, the Mayo Clinic's Dr. Wood remarked, "We found the need to develop [Mayo's applications] mostly on our own, because we have not found opportunities with partners who can develop them with us." Dr. Douglas Wood, Dept. of Med., Health Care Policy Research Group, Mayo Clinic, Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 169 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf). Another panelist noted that Marshfield Clinic has developed its core HIT systems since implementing its first eMR module in 1985. Thomas Berg, Dir. & Special Projects Manager, Clinical Info. Servs., Marshfield Clinic, Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 200–01 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf).

32. For example, Dossia is a consortium of large employers, including AT&T, Applied Materials, BP America, Inc., Cardinal Health, Intel Corporation, Pitney Bowes, Sanofi-Aventis, and Wal-Mart, who jointly developed and provide a PHR system for the voluntary use of their employees. A Dossia web site describing the consortium, its PHR, and its privacy policies is available at http://www.dossia.org/.

cies had devoted considerable resources to the development and promotion of HIT.[33]

Today, some large medical centers and health care systems are all but paperless, with systems at Marshfield Clinic, the Mayo Clinic, and Kaiser Permanente being described at some length at the FTC Workshop.[34] For example, Marshfield Clinic—which comprises about 45 health care facilities in Wisconsin and has integrated eHRs for about 2 million patients—reported that all specialties in its various clinics use the same integrated eHRs and that all inputs into the eHRs by the roughly 1200 physicians affiliated with Marshfield are done electronically.[35]

At the same time, the adoption of HIT, interoperability of HIT systems, and integration of health information has in many places lagged behind expectations.[36] In fact, paper–based patient record systems still dominate in U.S. medical practice, especially in small practice settings.[37] Only about four percent of U.S. physicians have access to a fully-functional eHR system, and only about thirteen percent have access to a

33. For example, although the ONC is established by statute under the Recovery Act, it initially was created to spearhead and integrate HIT initiatives in response to a 2004 executive order. 2004 Exec. Order, *supra* note 5.

34. Other systems, such as the Department of Veterans Affairs' (VA's) VistA system, also were discussed. *See, e.g.*, Berg, *supra* note 31, at 199–201 (discussing the Marshfield Clinic); Ferguson, *supra* note 25, at 134–35 (discussing Kaiser-Permanente); Dr. Robert M. Kolodner, Nat'l Coordinator, Health Info. Tech., Dep't. of Health & Human Servs., Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 293 (April 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf) (discussing the VA); Wood, *supra* note 31, at 169 (discussing the Mayo Clinic); *see also, e.g.*, GOV'T ACCOUNTABILITY OFFICE, GAO-04-0224, INFORMATION TECHNOLOGY, BENEFITS REALIZED FOR SELECTED HEALTH CARE FUNCTIONS 36 (Oct. 2003) (regarding Kaiser-Permanente), *available at* http:// www.gao.gov/new.items/d04224.pdf [hereinafter GAO 2003 REPORT]; *Id.* at 46–47 (regarding Mayo Clinic); *Id.* at 61–62 (regarding VA's VistA).

35. Berg, *supra* note 31, at 199–201.

36. "Despite the efforts of the National Committee on Vital and Health Statistics . . . and other groups, progress in health IT in the United States has been too slow." Robert M. Kolodner et al., *Health Information Technology: Strategic Initiatives, Real Progress*, HEALTH AFF. w391, w391-w392 (2008), http://content.healthaffairs.org/cgi/reprint/hlthaff.27.5.w391v1; *see also* CONG. BUDGET OFFICE, *supra* note 10, at 3 ("Despite the potential of health IT to increase efficiency and improve quality, though, very few providers as of 2006, about 12 percent of physicians and 11 percent of hospitals have adopted it"). *But cf.* Edward H. Shortliffe, *Strategic Action in Health Information Technology: Why the Obvious Has Taken So Long*, 24 HEALTH AFF. 1222, 1223 (2005) (examining slow growth in HIT "in context by assessing what has succeeded and what still remains to be realized, while asking what barriers exist that have prevented optimal progress to date").

37. David Gans et al., *Medical Groups' Adoption of Electronic Health Records and Information Systems*, 24 HEALTH AFF. 1323, 1325–26 (2005).

basic system.[38] According to one recent paper, "only 1.5% of U.S. hospitals have a comprehensive electronic–records system (i.e., present in all clinical units), and an additional 7.6% have a basic system (i.e., present in at least one clinical unit). Computerized provider–order entry for medications has been implemented in only 17% of hospitals."[39]

Indeed, the most basic policy issue in HIT may be the relative pace of its development and adoption. That is, given the public and private benefits anticipated with HIT—many of which have been observed in particular institutional settings—how is it that HIT markets are not more developed?[40] Why is HIT use not more common?

B. *Potential Benefits and Costs of HIT*

1. Benefits

Broadly, HIT benefits flow from two sources: stand–alone and network efficiencies.[41] Stand–alone efficiencies are those that accrue internally to an office, clinic, or hospital from its use of HIT, and may include reduced administrative and error costs. Network benefits are those that are realized *across* multiple health care service providers: when various parts of the health care system are able to communicate efficiently, each part enjoys increasing benefits as the scope of the network from which information may be drawn increases. In HIT such network benefits are likely to be more substantial than stand–alone benefits.[42] Most patients see multiple providers in a given year,[43] and providers often rely on external entities to perform lab and radiology work.[44] But, as the former National Coordinator for HIT has explained,

38. Catherine M. DesRoches et al., *Electronic Health Records in Ambulatory Care—A National Survey of Physicians*, 359 NEW ENG. J. MED. 50, 50 (2008) (basing these statistics on a national survey of 2,758 physicians).

39. Ashish K. Jha et al., *Use of Electronic Health Records in U.S. Hospitals*, NEW ENG. J. MED. 1628, 1628 (2009).

40. Many have been concerned about rates of adoption of HIT in different areas of health care; that is, substantially, a concern that demand has lagged behind expectations. In addition, however, there have been concerns that the supply of certain HIT utilities and HIT support services have been slow to meet demand. *See*, *e.g.*, Wood, *supra* 31, at 169; Berg, *supra* 31, at 200.

41. *See* Miller & Tucker, *supra* note 12, at 1080.

42. *See* David J. Brailer, *Interoperability: The Key to Future Health Care System*, HEALTH AFF. w5-19, w5-20 (2005), http://content.healthaffairs.org (use the search bar to locate the document and then follow the hyperlink).

43. *See* Hoffman & Podgurski, *supra* note 11, at 113 (reporting that the average Medicare patient visits seven different physicians in a given year); *see also* Brailer, *supra* note 42, at w5-19.

44. *See* Jan Walker et al., *The Value of Health Care Information Exchange and Interoperability*, HEALTH AFF. w5-0, w5-13–w5-14 (2005), http://content.healthaffairs.org (use the search bar to locate the document and then follow the hyperlink).

"[f]ragmentation . . . results in errors, duplication, lack of coordination, and many other problems."[45]

Although the flow of information should reduce fragmentation, the benefits of HIT on a national scale are very difficult to predict. As a CBO report has observed, "[n]o aspect of health IT entails as much uncertainty as the magnitude of its potential benefits."[46] A well–cited RAND report estimates that "effective EMR implementation could eventually save more than $81 billion annually."[47] Others have been critical of the RAND estimates.[48] The CBO, for example, has argued that the RAND study does not adequately distinguish between possible and likely benefits to HIT adoption, concluding that it is "not an appropriate guide to estimating the effects of legislative proposals aimed at boosting the use of health IT."[49] Such disputes may be difficult to resolve in any precise way in the short run. In brief, possible HIT benefits may be substantial, highly variable according to particular implementations, and otherwise uncertain.

At least locally, HIT has led to concrete qualitative improvements in health care services, according to process measures or outcome measures. One FTC Workshop panelist described, for example, a hospital system's adherence to the evidence–based process standard of ACE inhibitor prescription following myocardial infarction ("heart attack") upon discharge. In that case, implementation of evidence–based HIT clinical guidance at InterMountain Healthcare reportedly increased adherence to the standard from about 65% to about 95%—a process improvement—which reduced significantly the readmission rate—an

45. Brailer, *supra* note 42, at w5-19; *see also* Hoffman & Podgurski, *supra* note 11, at 113 (stating that when doctors do not communicate and coordinate a patient's care "any one of them may miss vital information that is critical to the individual's welfare").

46. CONG. BUDGET OFFICE, *supra* note 10, at 6.

47. Hillestad et al., *supra* note 6, at 1103.

48. CONG. BUDGET OFFICE, *supra* note 10, at 8–9 (claiming RAND overestimates probable benefits of HIT); *but cf.* David U. Himmelstein & Steffie Woolhandler, *Hope And Hype: Predicting The Impact Of Electronic Medical Records*, 24 HEALTH AFF. 1121, 1122 (2005) (arguing that the RAND analysis is a form of "hype" that "reveals a disturbing array of unproven assumptions, wishful thinking, and special effects"). We note that the RAND report's estimate is not generated by precisely the same problem as the CBO's critique of that estimate. Briefly, the RAND report addresses possible benefits of large-scale eMR adoption. Although the authors provide reasons to think that their estimate represents neither a "best case" nor a "worst case" scenario, they recognize that "the currently useful evidence is not robust enough to make strong predictions." Hillestad et al., *supra* note 6, at 1104–05. The CBO Report offers very useful analysis, but it does not offer any particular cost-benefit analysis attached to any particular legislative proposal, and like the RAND report, it does not appear to approach a comprehensive assessment of possible benefits (or costs) to HIT adoption.

49. CONG. BUDGET OFFICE, *supra* note 10, at 4.

outcome improvement.[50] That is consistent with survey data suggesting that physicians who employ eHRs report greater avoidance of costly medical errors, including, "having averted a known drug allergic reaction (80%) or a potentially dangerous drug interaction (71%), being alerted to a critical laboratory value (90%), ordering a critical laboratory test (68%) and providing preventive care (69%)."[51]

A 2003 General Accounting Office (GAO) Report, based on data from ten private and public health care delivery organizations, three insurers, and one community data network, described substantial efficiency gains in both administrative function and delivery of care across settings.[52] For example, Mayo Clinic, a 1,951–bed teaching hospital, achieved annual savings of about $8.6 million by replacing paper medical charts with electronic medical records for outpatients, $2.85 million by replacing manual medical record handling processes with electronic access to lab results and reports, $ 2.9 million by automating correspondence, and $7 million by reducing un–billable tests and billing patients directly.[53] Single–site studies have also been promising. For example, a study of the effects of eRx at Brigham and Women's Hospital indicated "large differences . . . for all main types of medication errors: dose errors, frequency errors, route errors, substitution errors, and allergies."[54]

50. Dr. Mark Dente, Vice President, Health Care Solutions & Integrated IT Solutions, GE Health Care, Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 277 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf) (describing HIT benefits at InterMountain Healthcare, a network of hospitals and clinics in Utah). Dr. Dente also described improvements in ventilator management with the implementation of evidence-based systems at InterMountain. In that case, he reported both significant improvement in the survival rate and a significant savings, approximately $120,000 per case, due to the implementation of HIT-based clinical support. *Id.* at 276–77.

51. DesRoches et al., *supra* note 38, at 54 (reporting on "fully functional" eHRs, although those with more basic systems reported "the same effects but less commonly").

52. *See generally*, GAO 2003 REPORT, *supra* note 34.

53. *Id.* at 46, 48.

54. David W. Bates et al., *The Impact of Computerized Physician Order Entry on Medication Error Prevention*, 6 J. AM. MED. INFORMATICS ASS'N. 313, 313 (1999); *see also, e.g.*, Hagop S. Mekhjian et al., *Immediate Benefits Realized Following Implementation of Physician Order Entry at an Academic Medical Center*, 9 J. AM. MED. INFORMATICS ASS'N. 529, 529, 539 (2002) (reporting that the joint introduction of computerized physician order entries (CPOEs) and eMR systems at Ohio State University Health System improved patient care by, for example, reducing turn-around times and eliminating all nursing and physician transcription errors); Kirsten Colpaert et al., *Impact of Computerized Physician Order Entry on Medication Prescription Errors in the Intensive Care Unit: A Controlled Cross-Sectional Trial*, 10 CRITICAL CARE R21 (2006), *available at* http://ccforum.com/content/10/1/R21 (reporting that HIT implementation in the ICU resulted in significant decreases in the occurrence and severity of medication errors).

At the same time, it is not clear from either the GAO Report or other studies that the reported efficiency gains represent *net* gains for the adopters. Also, although single–site studies demonstrating gains in clinical quality at academic medical centers are promising, results have been somewhat mixed, and there have been relatively few studies measuring qualitative gains using longitudinal national data. One recent study employing national data observes that EMRs "have a clear and statistically significant effect on patient safety," as they are associated with fewer infections attributable to medical care in hospitals, but that the observed effect is limited to one of the study's quality measures and, while "promising," is "small."[55] In addition, the promise of any gains may be at risk, as there have been significant problems with particular HIT implementations.[56]

Electronic prescribing illustrates both the potential benefits of HIT and the extent to which such benefits are uncertain prior to implementation. As noted above, eRx has long been considered an important and tractable area for HIT development and adoption. Preventable medication errors are numerous. The oft–cited 2006 IOM Report, PREVENTING MEDICATION ERRORS, for example, estimated that "at least 1.5 million preventable ADEs [adverse drug events] occur each year in the United States."[57] These errors inevitably impose medical costs, which, in turn, may impose substantial expense on private and public payers.[58]

The IOM Report suggested that eRx holds special promise for error avoidance,[59] and there are good reasons to agree. First, many errors

55. Stephen T. Parente & Jeffrey S. McCullough, *Health Information Technology and Patient Safety: Evidence from Panel Data*, 28 HEALTH AFF. 357, 358 (2009).

56. *See, e.g.*, Yong Y. Han et al., *Unexpected Increased Mortality After Implementation of a Commercially Sold Computerized Physician Order Entry System*, 116 PEDIATRICS 1506, 1506 (2005) (reporting an unexpected increase in mortality rates among children who were referred and admitted to the hospital after eRx implementation); Ross Koppel et al., *Role of Computerized Physician Order Entry Systems in Facilitating Medical Errors*, 293 J. AM. MED. ASS'N. 1197, 1198 (2005) (documenting errors associated with implementation of a widely-used, commercially-available computerized provider order entry system); Ceci Connolly, *Cedars-Sinai Doctors Cling to Pen and Paper*, WASH. POST, Mar. 21, 2005, at A01 (describing an unsuccessful attempt to implement a hospital-level electronic health record system and reporting that up to 30% of such implementations fail).

57. INST. OF MED., *supra* note 7, at 5.

58. *Id.* at 5, 132. That cost estimate excludes both errors of omission (cases where medication ought to have been prescribed and administered, but was not) and the larger economic costs—such as missed work days—imposed by preventable ADEs. The report noted that there are large gaps in our understanding of the costs of medication errors. *Id.* at 58. Nevertheless, the report also suggested that, for example, in-hospital adverse drug events alone might conservatively be estimated to cost $ 3.5 billion per year, in 2006 dollars. *Id.* at 132.

59. *Id.* at 229 ("By 2008, all prescribers should have plans in place to implement electronic prescribing."); *see also* Gilad J. Kuperman et al., *Medication-Related Clinical Decision Support in Computerized Provider Order Entry Systems: A Review*, 14 J. AM. MED.

appear to be caused by basic coding or information processing failures that should be amenable to automated control.[60] In addition, adverse events due to faulty drug or dose identity checking, failures in drug knowledge, and limited patient knowledge (i.e., patient history, current and recent medications, etc.),[61] should be reduced by eRx supported by eMRs and computerized drug information. In particular institutional settings, eRx has been associated with substantial reductions in preventable adverse drug events[62] and direct financial costs.[63]

On the other hand, there have been significant problems with particular implementations of eRx systems.[64] For example, although eRx implementation at the Children's Hospital of Pittsburgh appeared to reduce adverse drug events significantly during a nine–month study period,[65] a subsequent study of mortality rates among children who were referred and admitted to the hospital showed an unexpected increase in mortality after implementation.[66] Such problems seem to arise in transition to an eRx system, with incomplete or fragmented eRx systems, or with poor integration between training and practice standards on the one hand and the HIT systems on the other.[67] Those are not necessarily long–term, much less intractable, problems. Still, they suggest the potential for large transition costs in eRx adoption and may raise questions about the

INFORMATICS ASS'N. 29, 29 (2007) (reviewing literature and concluding that "CPOE . . . with clinical decision support . . . can improve patient safety and lower medication-related costs").

60. INST. OF MED., *supra* note 7, at 121–22 (errors include transcription errors, order-tracking errors, and inter-service communication errors).

61. *Id.*

62. *See, e.g.*, David W. Bates et al., *supra* note 54, at 313; Hagop S. Mekhjian et al., *supra* note 54, at 529, 539; Kirsten Colpaert et al., *supra* note 54.

63. *See, e.g.*, W.M. Tierney et al., *Physician Inpatient Order Writing on Microcomputer Workstations: Effects on Resource Utilization*, 269 J. AM. MED. ASS'N. 379, 379 (1993) (concluding that a network of microcomputer workstations for writing all inpatient orders significantly lowered patient charges and hospital costs); *cf.* David W. Bates et al., *The Costs of Adverse Drug Events in Hospitalized Patients*, 277 J. AM. MED. ASS'N. 307, 307 (1997) (discussing substantial costs of ADEs and preventable ADEs).

64. *See, e.g.*, Ceci Connolly, *supra* note 56, at A01 (describing an unsuccessful attempt to implement a hospital-level electronic health record system and reporting that up to 30% of such implementations fail).

65. Jeffrey S. Upperman et al., *The Impact of Hospitalwide Computerized Physician Order Entry on Medical Errors in a Pediatric Hospital*, 40 J. PEDIATRIC SURGERY 57, 57 (2005).

66. Han, *supra* note 56, at 1506; *see also, e.g.*, Koppel, *supra* note 56, at 1198 (claiming that the implementation of a widely-used and commercially-available CPOE system in an urban tertiary-care teaching hospital was associated with numerous categories of errors).

67. The JAMA-published study noted, for example, that medication errors were exacerbated in the system under study by the fact that patient medication records were shown in small fonts, across a large number of screens (up to 20), where patient names did not appear on all screens, as well as by "hectic" workstations and "common" crashes of the CPOE system. *See id.* at 1200–01.

extent to which efficiency gains realized in particular institutional settings can be generalized.[68]

2. Costs

One of the most obvious impediments to the adoption of HIT is its substantial cost. As discussed in the previous section, acquisition and implementation of HIT systems are costly, operating and maintenance costs are ongoing, and HIT investments may be regarded as at–risk. Regulatory costs, uncertainty, "cultural" aversions to HIT, and concerns about liability exposure also are likely to slow adoption. And yet, as one FTC Workshop panelist succinctly stated with respect to HIT investments, "there is no billing code for it."[69]

HIT adoption costs are varied and substantial. The CBO has noted that adoption costs include: (1) the initial fixed cost of the hardware, software, and technical assistance necessary to install the system, (2) licensing fees, (3) the expense of maintaining the system, and (4) the "opportunity cost" of the time that health care providers could have spent seeing patients but instead must devote to learning how to use the new system and how to adjust their work practices accordingly.[70] Although the data is limited, and there is some evidence HIT system prices are falling, recent studies suggest that, (a) physicians' offices may be expected to pay initial costs of $25,000–$45,000 to acquire an office–based HIT system;[71] (b) annual operating costs are 12–20% of initial cost;[72] (c) implementation costs for hospitals range from $3 million for

68. *See* Salomeh Keyhani et al., *Electronic Health Records and the Quality of Care*, 46 MED. CARE 1267 (2008). In this study, the authors conducted cross-sectional analyses of national data gathered in ambulatory care settings, including physician offices. Examining blood pressure control in particular, the authors generally failed to find a relationship between eHR adoption and the examined quality of care measures, and concluded that "[i]t is doubtful that presence of an EHR alone can improve the quality of care." *Id.* at 1270; *see also* Jeffrey A. Linder, et al., *Electronic Health Record Use and the Quality of Ambulatory Care in the United States*, 167 ARCHIVES OF INTERNAL MED. 1400, 1400 (2007) (failing to find quality improvements, on most measures, associated with eHRs as implemented in ambulatory care settings). *But cf.* DesRoches et al., *supra* note 38, at 50 (discussing quality improvements reported by ambulatory care providers).

69. Ferguson, *supra* note 25, at 195. There have long been concerns about misaligned payment incentives in health care markets associated with third-party payment and regulation. *See, e.g.*, F.T.C. & DEP'T OF JUSTICE, IMPROVING HEALTH CARE: A DOSE OF COMPETITION, Exec. Summ. 5 (2004), *available at* http://www.ftc.gov/reports/healthcare/040723healthcarerpt.pdf [hereinafter A DOSE OF COMPETITION]. For example, as the FTC/DOJ Report observes, "Government administered pricing by CMS inadvertently can distort market competition . . . . CMS never decided as a matter of policy to provide greater profits for cardiac surgery than many other types of service, but the [payment system] . . . tends to do so." *Id.* at Exec. Summ. 16.

70. CONG. BUDGET OFFICE, *supra* note 10, at 17.

71. *Id.*

72. *Id.*

smaller hospitals to $7.9 million for large hospitals;[73] and (d) average hospital operating costs are about 19% of one–time costs, or $2,700 per bed.[74] CBO and others also have observed substantial operating costs associated with HIT.[75]

It appears that cost structures co–vary with rates of HIT adoption by type and size of practice setting. For example, "[l]arge hospitals (200 beds or more) have three to four times greater adoption rates than those of smaller hospitals (fewer than 50 beds),"[76] which may be due, in part, to the ability of larger facilities to "take advantage of economies of scale by spreading the fixed costs of health IT over a larger base."[77] Academic medical centers also have relatively high adoption rates,[78] perhaps because certain HIT costs may be shared with (and are especially valuable to) research and teaching functions of the hospitals.[79] Adoption rates also vary according to practice size in group practice settings, with small practice groups (5 full–time physicians or fewer) having the lowest rate of eHR adoption and the highest percentage of paper medical records.[80]

Large medical centers also have expressed concerns about costs resulting from the interruption or restructuring of work flow.[81] The integrated HIT system implemented at the Mayo Clinic may be considered a success in many ways. At the same time, Mayo acknowledges that its eMR has "had its share of problems because it didn't really match the physician workflow."[82] In some ways, such costs are among the various "cultural" barriers to HIT adoption, which have to do with providers' and patients' comfort levels with HIT. For example, HIT may influence the

73. *Id.* at 18.

74. *Id.*

75. With regard to small offices, "[e]stimates of annual costs for operating and maintaining the system . . . range between about 12 percent and 20 percent of initial costs." *Id.* (citing Robert H. Miller et al., *The Value of Electronic Health Records in Solo or Small Practices*, 24 HEALTH AFF. 1127 (2005); Samuel J. Wang et al., *A Cost-Benefit Analysis of Electronic Medical Records in Primary Care*, 114 AM. J. MED. 397 (2003)). Hospital operating costs vary by size and type of hospital but are estimated to be about 19% of acquisition costs, or $2,700 per bed. CONG. BUDGET OFFICE, *supra* note 10, at 18.

76. Michael F. Furukawa et al., *Adoption of Health Information Technology for Medication Safety in U.S. Hospitals, 2006*, 27 HEALTH AFF. 865, 868 (2008).

77. *Id.* at 867.

78. *Id.* at 868.

79. *Id.* at 867.

80. *See, e.g.*, Gans et al., *supra* note 37, at 1323, 1325. Also, "[b]ecause of the structure of the tax code, most practices do not have retained earnings, and, consequently, the capital equipment expenditures are funded directly from physician income." *Id.* at 1329.

81. *See, e.g.*, Dr. Kevin Carr, Physician Senior Manager for Clinical Transformation Health Care, BearingPoint, Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 153–54 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf); Kolodner, *supra* note 34, at 294; Wood, *supra* note 31, at 177.

82. Wood, *supra* note 31, at 171.

way health care professionals collaborate and interact, in addition to the way they keep and consult records and reference outside sources;[83] it may also influence the nature of patient/provider interactions.[84] As one FTC Workshop panelist explained, in many smaller practices, providers may be especially likely to face the question "how ready and willing am I to change the things that I do every single day"?[85]

Patients also may be wary of the ability of HIT systems to protect their sensitive information. For example, survey data suggests that a large proportion of consumers have concerns about the adequacy of extant privacy protections for their medical records and about the risks that may be presented by inadequate privacy protections.[86] Consumer apprehension about HIT can affect adoption rates of consumer–oriented HIT products, such as PHRs. It also may reduce demand–side pressures for providers to adopt HIT.[87]

The economic benefits of HIT adoption are thus uncertain, and HIT investments generally have been regarded as at–risk investments, potential benefits notwithstanding. Uncertainty reduces the present value of future HIT benefits, and thus private incentives for providers to adopt HIT. As noted above, implementation may be difficult and clinical improvements may be uncertain. Expected benefits are likely to be a positive function of one system's ability to communicate with others, but providers may be unsure whether a system they adopt today will prove to

83. *See, e.g.*, Ferguson, *supra* note 25, at 138–39.

84. *Id.*

85. Carr, *supra* note 81, at 154; *see also* Gans et al., *supra* note 37, at 1325–26.

86. *See, e.g.*, McGraw, *supra* note 31, at 142 ("[T]he survey data is also very clear that people have significant concerns about the privacy of their medical records, particularly in electronic form."); *see also* Wood, *supra* note 31, at 184 (regarding Mayo Clinic surveys of patient privacy concerns); Joy Pritts, Dir. for the Center of Med. Record Rights and Privacy, Health Policy Inst., Georgetown Univ., Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 287–88 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf); WESTIN, *supra* note 20, at 15 (providing nationwide survey data that suggests 58% believe medical record privacy is insufficiently protected); MARKLE FOUND., AMERICANS OVERWHELMINGLY BELIEVE ELECTRONIC PERSONAL HEALTH RECORDS COULD IMPROVE THEIR HEALTH (2008), *available at* http://www.connectingforhealth.org/resources/ResearchBrief-200806.pdf; CAL. HEALTHCARE FOUND., THE STATE OF HEALTH INFORMATION TECHNOLOGY IN CALIFORNIA: CONSUMER PERSPECTIVE 2 (2008), *available at* http://www.chcf.org/documents/chronicdisease/HITConsumerSnapshot08.pdf (stating that a survey of California health care consumers shows "most consumers in California are wary about using health information technology (HIT), such as personal health records (PHRs)" although many consumers are interested in HIT and use the Internet for health information); NATIONWIDE SUMM., *supra* note 13, at 6-36.

87. McGraw, *supra* note 31, at 195 ("But the improvements in health care quality and the cost reductions . . . that are there as potentials, are going to drive the other actors in the system, consumers and purchasers . . . to actually be on the demand side [of HIT adoption]."); *Cf.* Ferguson, *supra* note 25, at 138–39 (discussing popularity, among Kaiser consumers, of secure online communications with providers, online appointment scheduling, online lab results, and online Rx refills).

be "the right product"—one that will be interoperable tomorrow.[88] Interoperability standards, or more developed certification, may help to ameliorate such concerns, at least for some providers.[89] Providers also have expressed concern about potential liability arising from the mishandling of patient information *after* it leaves their offices in electronic form.[90]

In addition, although the interconnection and interoperability of nodes in an adequately large network may be prerequisites to the flow of health information, they cannot guarantee it. First, the extent to which different providers see clinical utility in the free flow of health information is likely to vary. Second, at the FTC Workshop, panelists suggested that some providers may worry that interoperable HIT can facilitate "business going out the door;"[91] among other things, it may lower the switching costs for patients who wish to switch providers, who may be disinclined to reduce the preference (or lock–in) that their patients have for them. Although federal law generally requires that consumers be provided access to, and copies of, their medical records,[92] access may be seen as costly if copies can be obtained only (a) within thirty days, (b) following a written request, and (c) with a copying fee—perhaps especially if a consumer's record is fragmented and distributed across different providers. Lowering the costs of the flow of information may generally be beneficial for consumers and competition, but it is not necessarily beneficial for all competitors.[93] This may partly explain why the actual flow of usable electronic health information between providers appears low even in the context of limited eHR adoption. That is, it may be that the problem of making a business case for the adoption of interoperable HIT systems can be, and often is, parsed from the problem of

88. Ferguson, *supra* note 25, at 192 (stating that providers prefer "a sense of comfort or trust that they are buying the right product, that they are spending their limited resources on things that they can use to get to a very basic level of coordination of care for their patients").

89. To the extent that some of the signal successes of HIT development have been realized in proprietary systems developed and implemented by certain large, sophisticated health care providers, further questions might be raised about the extent to which developing national standards (and certification standards) may or may not impose heightened costs (or, potentially, advantages) on certain established players.

90. *See* NATIONWIDE SUMM., *supra* note 13, at 6-36 to 6-37.

91. McGraw, *supra* note 31, at 195; *cf.* Carr, *supra* note 81, at 194 (discussing provider concerns about lost business as difficult to overcome and appeals that have been successful in overcoming it).

92. *See* 45 C.F.R. § 164.524(a) (2010).

93. Further, to the extent that HIT reduces consumers' switching costs, it may make them more likely to comparison shop for providers. If so, price and quality transparency may become more valuable. There could be a parallel issue for labor markets for health care professionals. Reducing the cost of transferring a consumer's health care information might also reduce the costs of changing employment or other business arrangements for that consumer's caregivers.

making a case for the sharing of health information via such systems—something policy makers might keep in mind to the extent that the first problem is solved via subsidies for adoption alone or adoption coupled with narrow usage criteria.

The substantial costs associated with adoption would not necessarily represent an intractable barrier if providers could capture fully the benefits of their HIT investments; market forces should encourage the adoption of efficient systems over time. However, although health care providers clearly capture some of those benefits, many remain externalized.[94] Hence, private incentives to adopt HIT are likely lower than those that would be socially efficient. As one FTC Workshop panelist explained, "You always have the debate, why do I have to pay it because it is everybody else who benefits, so they should pay."[95] This incentive problem is due primarily to two factors: (1) typically providers are not rewarded financially for improvements in efficiency and quality of care, and (2) HIT is subject to network effects. In network industries—discussed in Part III, *infra*, of this Article—consumers do not fully capture the benefits of their own consumption and hence may tend to under–invest in that consumption. A tertiary category of benefits, related to both of these, is that of public health benefits to which HIT adoption and information sharing may substantially contribute; these benefits are necessarily distributed across the larger society.

Providers generally capture certain benefits due to improved productivity. For example, if systems permit them to see more patients or perform a larger volume of procedures per unit time, the providers themselves are likely to benefit. Providers are not likely, however, to capture many of the HIT-enabled benefits of improved patient outcomes or improved public health.[96] Although reputational assets may be valuable in medicine, payment and reimbursement arrangements generally do not compensate providers for improved quality of care. For example, reducing the duplication of diagnostic tests benefits patients and insurers in the form of lower payments, less inconvenience, and, with certain testing procedures,

94. Miller, *supra* note 21, at 224 ("stand-alone provider benefit"); *see also* CONG. BUDGET OFFICE, *supra* note 10, at 20 ("Other benefits, such as lower costs for maintaining medical records and transcribing clinical data, clearly accrue to the provider who purchases the health IT system.").

95. Paul Uhrig, Gen. Couns. & Exec. Vice President of Corp. Dev., Chief Privacy Office, SureScripts, Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 181 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf).

96. Of course, reputational benefits, among others, may accrue to providers that improve their outcomes, but to the extent that the quality and availability of comparative health care quality information remains poor, such reputational benefits are likely to be muted.

reduced patient risk.[97] But on average, these social benefits actually reduce payments to providers. Further, although Medicare, Medicaid, and some private insurers have begun to implement limited pay–for–performance or other quality–based incentive programs, the financial gains associated with quality improvements are typically modest. By and large, providers are not compensated for qualitative improvements in care and limited countervailing programs are unlikely to tip the balance in favor of HIT investment.[98]

Underinvestment due to the inability of providers to capture the full benefits of their HIT investments could be ameliorated if such investments were subsidized, which is exactly what the Recovery Act does. For example, under Medicare, subject to certain constraints and obligations, eligible health care professionals may be eligible for up to five years of incentive payments, in amounts decreasing from $15,000–$18,000 for the first year;[99] hospitals may be eligible for incentive payments over a four year period, beginning with first year payments that include base payments of $ 2 million.[100] Most incentives are structured to encourage relatively early adoption of interoperable HIT (and, correspondingly, to discourage failures to adopt).[101] In addition, interspersed throughout the Act are direct and indirect incentives to spur the development and implementation of HIT through funding initiatives directed to various other federal agencies and federal grants to and through the states.[102]

97. *See* CONG. BUDGET OFFICE, *supra* note 10, at 19–20.

98. *See id.* at 20.

99. American Recovery and Reinvestment Act of 2009 (Recovery Act), Pub. L. No. 111-5, § 4101(a), 123 Stat. 115, 238 (2009) (providing reimbursement amounts varying according to the year in which payments begin and a 10% increase for professionals providing services in designated shortage areas). Hospital-based professionals may be excluded from such incentive payments under the Section as hospitals separately are eligible for incentive payments.

100. Such payments begin with a base payment of $2 million in the first year—plus an amount that varies according to a hospital's number of patient discharges in the payment year—and decrease progressively each year. *Id.* § 4102. Varied incentive payments are also provided for under the Medicaid program. *Id.*

101. Incentives are in several regards time-sensitive. First, direct financial incentive payments are not available past a certain threshold: "No incentive payments may be made under this subsection with respect to a year after 2016." *Id.* § 4101(a). "If the first payment year for an eligible professional is after 2014 then the applicable amount . . . for such professional for such year and any subsequent year shall be $0." *Id.* Furthermore, the statute provides for certain reductions in scheduled fee payment amounts, for services provided under Medicare, for an eligible provider who is "not a meaningful EHR user" in 2015 and subsequent years. *See id.* § 4101(b).

102. *See, e.g.* Recovery Act div. A, tit. I & div. B, tit. VI (directing the Assistant Secretary of Commerce and the FCC to expand nationwide broadband service and providing $2.5 billion in grants to the Department of Agriculture for the expansion of high-speed broadband service in rural communities, both courses being likely to impact access to HIT technology

For many health care providers, these programs may tip the balance in favor of HIT adoption.[103] This is, however, a form of industrial planning on a grand scale and a short clock, and it is unclear whether ARRA programs are properly calibrated to address the apparent market failure. Planned subsidies will be adequate, inadequate, or excessive responses to adoption shortfalls associated with current reimbursement policies.

Additional barriers to HIT, or costs associated with its adoption, include, among others, regulatory costs and network effects, which we discuss below.

C. *Federal and State Health Information Privacy and Data Security Law*

Three primary sources of privacy regulation apply to HIT. First, HHS administers HIPAA and its associated Privacy and Data Security Rules. Second, the FTC enforces the FTC Act against entities that fail to safeguard sensitive information. Finally, states have their own privacy and data security laws. Additional regulation is emerging under the Recovery Act.[104]

1. HIPAA

Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996, in part for the purpose of improving "the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the

---

nationwide); *see also id.* at div. A, tit. II (providing $4.7 billion in grants to expand broadband technology in order to increase, among other things, public access to computer technology, which will broaden access to HIT); *id.* at div. A, tit. VII (providing $85 million to Indian Health Services and $415 million toward improving Indian Health Facilities; portions of each will involve purchasing equipment that will improve access to HIT); *id.* at div. A, tit. VIII (providing $1 billion to the National Center for Research Resources to renovate and repair non-federal research facilities, some which will require upgrades for HIT); *id.* (providing the Agency for HealthCare Research and Quality with $700 million for comparative effectiveness research, with a portion likely to be targeted at price and quality transparency and/or HIT-related research).

103. It should also be anticipated that such programs will have an effect on private development of HIT applications and services. For example, it was recently reported that Wal-Mart intends to market electronic health records to physicians in small office practices. *See* Steve Lohr, *Wal-Mart to Digitize Health Data*, N.Y. TIMES, Mar. 11, 2009, at B1.

104. *See, e.g.*, FTC Notice of Proposed Rulemaking, 74 Fed. Reg. 17,914 (April 20, 2009) (to be codified at 16 C.F.R. pt. 318) (proposed rule under Recovery Act); *see also* Dep't of Health & Human Servs., Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009, 74 Fed. Reg. 19,006 (Apr. 27, 2009) (to be codified at 45 C.F.R. pts. 160 and 164).

establishment of standards and requirements for the electronic transmission of certain health information."[105] Among other things, HIPAA and its implementing regulations provide certain assurances to individual health care consumers about the privacy of their medical information.[106]

The Administrative Simplification provisions of HIPAA[107] have led HHS to promulgate a suite of rules,[108] with one, the Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule or the Rule), bearing particular significance for privacy concerns associated with HIT.[109] The Privacy Rule applies to protected health information (PHI), which is individually–identifiable health information that is "held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral."[110] HHS also promulgated a rule concerning security standards (the Security Rule), which requires reasonable and appropriate administrative, physical, and technological safeguards to ensure the integrity and confidentiality of PHI that is in electronic form.[111] The Security Rule complements the Privacy Rule: among other things, certain elements of data security may be viewed as

105. Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1302d note (2008).

106. In particular, the HIPAA Privacy Rule provides those assurances to individual human persons who are the end-consumers of health care. 45 C.F.R. § 160.103 (2002) ("Individual means the person who is the subject of protected health information.").

107. 42 U.S.C. § 1320d.

108. HHS has promulgated the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, Unique Identifiers Rules, and the Enforcement Rule.

109. The Privacy Rule initially was promulgated in December 2000. *See* Dep't of Health & Human Servs., Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82,462 (Dec. 28, 2000). It became effective in April 2001. *See* Dep't of Health & Human Servs., Standards for Privacy of Individually Identifiable Health Information, Final Rule; Correction of Effective and Compliance Dates, 66 Fed. Reg. 12,434 (Feb. 26, 2001). Modifications to the Rule were published in the Federal Register in August 2002 and became effective in October of that year. Dep't of Health & Human Servs., Standards for Privacy of Individually Identifiable Health Information, Final Rule, 67 Fed. Reg. 53,182 (Aug. 14, 2002). The Privacy Rule is codified at 45 C.F.R. pts. 160, 164. It should be noted that the compliance date for most covered entities under the rule was not until April 14, 2003. 45 C.F.R. § 164.534 (2010).

110. DEP'T OF HEALTH & HUMAN SERVS., OCR PRIVACY BRIEF: SUMMARY OF THE HIPAA PRIVACY RULE 3 (2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. [hereinafter HHS PRIVACY RULE SUMM.]. For regulatory definitions of health information, individually identifiable health information, and protected health information, see 45 C.F.R. § 164.103 (2003).

111. Health Insurance Reform: Security Standards, Final Rule ("The HIPAA Security Rule"), 68 Fed. Reg. 8,334 (Feb. 20, 2003) (codified at 45 C.F.R. pt. 160 and Subparts A and C of pt. 164). HHS promulgated the Security Rule, like the Privacy Rule, to implement certain HIPAA statutory provisions, with enforcement of the Privacy Rule being chiefly the responsibility of the HHS Office of Civil Rights (OCR) and enforcement of the Security Rule being chiefly the responsibility of CMS.

implementations of privacy policies codified in HIPAA and the Privacy Rule.

Several features of HIPAA are especially salient to the present discussion. First, the Privacy Rule establishes circumstances in which use or disclosure by a covered entity or business associate is permitted.[112] Covered entities generally may use or disclose PHI, without authorization, as follows: (1) to the individual subject of that information; (2) for treatment, payment, and health care operations; (3) incident to an otherwise permitted use and disclosure; (4) for certain public interest and benefit activities; and (5) as limited data sets for research, health care operations, or public health purposes.[113] Second, when use or disclosure of information is not expressly permitted, a covered entity generally must obtain written authorization from the individual prior to such use or disclosure.[114] Third, HIPAA and the Rule establish a federal floor of protection for individually–identifiable health information, at least with regard to covered entities,[115] in general, leaving the states free to adopt more stringent protections for consumers than those guaranteed under federal law.

The Recovery Act generally maintains HIPAA's privacy and data security requirements, to the extent that they are consistent with pertinent provisions of the Recovery Act itself,[116] as well as HHS authority under HIPAA.[117] In addition, the Recovery Act expands upon consumer privacy protections already contemplated under HIPAA. For example, under HIPAA, business associates of covered entities were subject chiefly to indirect regulation: covered entities were required to impose certain contractual limits on the use and disclosure of PHI by their business associates, but those limits were not generally subject to HHS enforcement or to private actions by the individual health care consumers whose PHI might be at issue but who were not themselves in privity with the business associates.[118] The Recovery Act provides for the direct

112. 45 C.F.R. § 164.502(a)(1) (2008).

113. *Id.* at 164.502(a)(1) (2008); DEP'T OF HEALTH & HUMAN SERVS., OCR PRIVACY BRIEF: SUMMARY OF THE HIPAA PRIVACY RULE 1–2 (2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. [hereinafter HHS PRIVACY RULE SUMM.].

114. 45 C.F.R. § 164.508 (2002).

115. HHS PRIVACY RULE SUMM., *supra* note 113, at 1–2.

116. American Recovery and Reinvestment Act of 2009 (Recovery Act), Pub. L. No. 111-5, § 13421, 123 Stat. 115, 238 (2009).

117. *Id.* § 3009(a).

118. This had been identified as one of the significant "gaps" in HIPAA coverage by panelists at the FTC Workshop and other commentators. *See* Susan McAndrew, Deputy Dir. for Health Info. Privacy, HHS Office of Civil Rights, Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 211 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf) (regarding "certain gaps in

application of certain security and privacy provisions to parties that, under HIPAA, are business associates of covered entities.[119] The Recovery Act also regulates the use and disclosure of PHI by certain non-HIPAA-covered entities, such as vendors of PHRs and third parties that offer products or services through the web sites of vendors of PHRs.[120]

2. The FTC Act

A provider can violate the FTC Act's prohibition on deceptive acts by making false or misleading promises to patients that it will safeguard their data. Additionally, a provider can violate Section 5 of the FTC Act by failing to take reasonable steps to safeguard patients' data that cause, or are likely to cause, significant consumer harm.[121] Since 2001, the FTC has obtained twenty–two consent orders against companies that allegedly failed to provide reasonable protections for sensitive consumer information in violation of Section 5.[122]

In 2002, for example, Eli Lilly allegedly released the names and e–mail addresses of more than 650 individual Prozac consumers, who had voluntarily registered, via a Lilly web site, to receive prescription refill reminders.[123] Because the disclosures appeared to violate Lilly's own published privacy and data security assurances[124] to the detriment of the consumers who had registered with Lilly under that policy, the disclosures prompted an FTC investigation. That investigation concluded with a settlement, including a consent order that prohibits false or misleading privacy statements and commits the company to implement certain privacy protections going forward.[125] More recently, CVS Caremark agreed to settle charges that it had failed, in violation of the FTC Act, to take

---

the current HIPAA coverage"); Pritts, *supra* note 86, at 289 (describing "gaps" in federal and state privacy protections as difficult to identify and needs for consumer control and trust not being met).

119. *Recovery Act* §§ 13401, 13404 (outlining application of security provisions and penalties and application of privacy provisions and penalties, respectively).

120. *Id.* § 13407. Treatment of PHR-related entities also has been identified as a gap in HIPAA coverage. McGraw, *supra* note 31, at 146–47 (regarding "gaps" in HIPAA coverage, especially with regard to personal health records).

121. *See In re* CVS Caremark Corp., F.T.C. File No. 072-3119, Comp. (February 18, 2009).

122. *See*, *e.g.*, F.T.C. v. Navone, No. 2:08-CV-01842 (D. Nev. Dec. 30, 2008); U.S. v. ValueClick, Inc., No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008*); In re* Eli Lilly & Co., F.T.C. Docket No. C-4047 (May 8, 2002).

123. Press Release, F.T.C., Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* http://www.ftc.gov/opa/2002/01/elililly.htm.

124. *Id.*

125. *In re* Eli Lilly & Co., File No. 012 3214, Agreement Containing Consent Order (Jan. 18, 2002), *available at* http://www.ftc.gov/os/2002/01/lillyagree.pdf; *see also In re* Eli Lilly & Co., File No. 012 3214, Decision and Order (May 10, 2002), *available at* http://www.ftc.gov/os/2002/05/elililly do.htm.

reasonable and appropriate security measures to protect sensitive financial and medical information of its customers and employees.[126]

The Recovery Act has given the FTC more specific responsibility in the HIT privacy arena, particularly in its breach notification provisions. One set of ARRA breach notification requirements—to be enforced by HHS—pertains to HIPAA–covered entities such as health care providers; another—to be enforced by the FTC—pertains to certain non–HIPAA–covered entities, such as vendors of PHRs and their affiliated third–party service providers.[127] Vendors of PHRs and related entities that discover certain PHI security breaches are required to notify both the FTC and the consumer whose PHI was breached.[128]

3. State Law

A substantial body of state regulation exists regarding the privacy and security of consumer health information.[129] As we have said, HIPAA and the Privacy Rule establish a federal floor of protection for individually–identifiable health information, at least with regard to covered entities, leaving the states free to adopt more stringent protections for consumers than those guaranteed under federal law.[130] As a result, "states

126. CVS Caremark, F.T.C. File No. 072-3119 (claiming that respondent allegedly "discarded materials containing personal information in clear readable text (such as prescriptions, prescription bottles, pharmacy labels, computer printouts, prescription purchase refunds, credit card receipts, and employee records) in unsecured, publicly-accessible trash dumpsters on numerous occasions"). CVS Caremark independently agreed to pay $2.25 million to resolve HHS allegations that it violated HIPAA. *Id.*

127. American Recovery and Reinvestment Act of 2009 (Recovery Act), Pub. L. No. 111-5, § 13407, 123 Stat. 115, 238 (2009).

128. The FTC is required to notify HHS in turn. The requirements pertain to "(i) vendors of personal health records; (ii) entities that offer products or services through the website of a vendor of personal health records; (iii) entities that are not covered entities and that offer products or services through the websites of covered entities that offer individuals personal health records; (iv) entities that are not covered entities and that access information in a personal health record or send information to a personal health record; and (v) third party service providers used by a vendor or entity described in clause (i), (ii), (iii), or (iv) to assist in providing personal health record products or services" (incorporating entities described under the Recovery Act § 13424(b)(1)(A) by reference). The section also requires the FTC to promulgate certain interim final regulations to enforce this provision. *Id.* § 13424; *see also* F.T.C., Notice of Proposed Rulemaking; Request for Public Comment, re 16 C.F.R. Pt. 318, Health Breach Notification Rule, 74 Fed. Reg. 17,914 (Apr. 20, 2009).

129. *See generally*, *e.g.*, Dimitropoulos & Rizk, *supra* note 14, at 428–29 (issues in accommodating state-level variation); NATIONWIDE SUMM., *supra* note 13, at 6-3. For a general overview of state law provisions, *see* INST. FOR HEALTH CARE RESEARCH & POLICY, GEORGETOWN UNIV., JOY L. PRITTS ET AL., THE STATE OF HEALTH PRIVACY: A SURVEY OF STATE HEALTH PRIVACY (2d ed. 2003), *available at* http://hpi.georgetown.edu/privacy/pdfs/statereport2.pdf (last visited March 31, 2010) [hereinafter PRITTS ET AL., 2003] (summarizing health privacy statutes circa 2002 for all fifty states plus District of Columbia).

130. Congress intended for HIPAA to serve as a federally-mandated *floor* of protection for PHI, rather than a *ceiling*. Accordingly, state legislatures can further regulate the use and

have a wide variety of protections for personal health information. Some are at, or very close to, the floor of the HIPAA Privacy Rule, while others impose much more restrictive measures."[131] Although it sometimes may be difficult to determine which jurisdiction's requirements are more stringent, the Privacy Rule does provide some guidance in that regard.[132]

In that context, many states have maintained health privacy protections in the wake of HIPAA, with the particulars varying substantially from state to state.[133] Some states have reduced the scope of their own health information privacy and security regulation, some have sought to recapitulate federal protections, and some have increased the scope or strength of their regulations.[134] States regulate, among other things, procedural access provisions, condition-specific disclosure rules, and causes of action for access and disclosure violations.[135] States may also establish forms of physician–patient privilege, general rights of health privacy, and the assignment of property rights in medical files to patients. Privacy and data security remain active areas of state regulatory activity, and several states have taken recent steps to make their regulations regarding

disclosure of PHI. 67 Fed. Reg. at 53,182. In general, state laws that are contrary to the HIPAA Privacy Rule are preempted by the federal requirements. 45 C.F.R. § 160.203. A state law is "contrary" to the Privacy Rule if it would be impossible to comply with both the state and federal requirements, or if the state law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA. 45 C.F.R. § 160.202. However, if a provision of state law is more stringent than a provision of the Privacy Rule, and it is possible to comply with both the state law and the Privacy Rule, there is no conflict between the state law and the Privacy Rule and no preemption.

131. NATIONWIDE SUMM., *supra* note 13, at 6-13.

132. A state law is "more stringent" if it, among other things, further restricts a use or disclosure otherwise permitted under the Privacy Rule, "provides greater privacy protection for the individual who is the subject of the [PHI]," or provides the individual health care consumer with either a greater right of access to her PHI or a more detailed accounting of use and disclosure of her PHI. 45 C.F.R. § 160.202. The 4th Circuit has upheld HIPAA's nonpreemption provision against claims that it violates the Due Process Clause of the Fifth Amendment for vagueness, finding that, although the "criteria will doubtless call for covered entities to make some common sense evaluations and comparisons between state and federal laws, [it] does not mean they are either vague or constitutionally infirm." South Carolina Med. Ass'n v. Thompson, 327 F.3d 346, 355 (4th Cir. 2003).

133. *See generally, e.g.*, Dimitropoulos & Rizk, *supra* note 14; PRITTS ET AL., 2003, *supra* note 129.

134. *See* 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, 345–47 (2002) (reviewing state policy changes since HIPAA generally and comparing, e.g., Hawaii, which repealed its state health privacy statute in response to the Rule, and Texas, which "adopted a broad health privacy statute that both mirrors and expands upon the Federal Health Privacy Rule").

135. *See generally id.*

medical privacy and data security more stringent. For example, California enacted two pieces of health information legislation in 2008.[136]

Other states have adopted general regulations on personally identifiable information that sweep broadly enough to have implications for HIT entities. For example, Massachusetts adopted "Standards for the Protection of Personal Information of Residents of the Commonwealth," which "apply to all persons that own, license, store or maintain personal information about a resident of the Commonwealth."[137]

Many state law provisions revisit or replicate federal standards. For example, federal law generally provides individual health care consumers with certain rights of access to their medical records, requiring that health care providers furnish such access within 30 or 60 days, depending on the particulars of the consumer request.[138] Certain states have adopted requirements that mirror the federal 30 and 60-day response times.[139] Other states provide for rights of access, but require that health care providers act more quickly than required under federal law.[140] Still other states provide for access to medical records under more particular circumstances, such as telemedicine[141] or ambulance

136. *See generally* Assemb. Bill 211, An Act to Amend § 56.36 of the CAL. CIV. CODE, and to Add Division 109 (Commencing with § 130200) to the CAL. HEALTH & SAFETY Code, Relating to Health (approved by Governor Sept. 30, 2008); Senate Bill No. 541, An Act to Amend §§ 1280.1 and 1280.3 of, and to Add § 1280.15 to, the CAL. HEALTH & SAFETY CODE, Relating to Health Facilities (approved by Governor Sept. 30, 2008). Among other things, these (a) require health care providers and other entities to adopt safeguards against the unauthorized disclosure of consumer health records, Ca. A.B. 211 § 2 (CAL. HEALTH & SAFETY CODE § 130203(a)), (b) make certain violations of medical privacy punishable as misdemeanors, establishing private and public remedies for unauthorized disclosures, including private rights of action, administrative fines, and civil penalties, *id.* § 1 (CAL. CIV. CODE § 56.36(a)–(c)) and Cal. S.B. No. 541 §§ 1–3 (CAL. HEALTH & SAFETY CODE §§ 1280.1, 1280.15, & 1280.3), and (c) require prompt reporting of unauthorized disclosures of protected health information to both the state and the individual consumers whose information is disclosed, Cal. S.B. No. 541 § 2 (CAL. HEALTH & SAFETY CODE § 1280.15(b)(1)–(2)).

137. 201 C.M.R. §§ 17.00–17.01. Section 17.01 regards purpose and scope.

138. *See* 45 C.F.R. § 164.524(b)(2).

139. *See, e.g.*, 735 ILL. COMP. STAT. 5/8-2001(e) (2008).

140. For example, South Carolina law allows 45 days for the requisite disclosures, while Maryland only allows 21, Louisiana, among others, allows 15, Wyoming allows 10, and California allows as few as 5. S.C. CODE ANN. § 44-7-325 (2007); MD. CODE ANN., HEALTH-GEN. § 4-309(a) (2008); LA. REV. STAT. ANN. § 40:1299.96 (2008); WYO. STAT. ANN. § 35-2-611 (2008); CAL. HEALTH & SAFETY CODE §§ 123110, 123130 (2007). *See also* WASH. REV. CODE ANN. § 70.02.080 (2008) & TEX. HEALTH & SAFETY CODE § 241.154 (2007) (additional state statutes requiring disclosure within 15 days).

141. *See* CAL. HEALTH & SAFETY CODE § 123149.5 (2007) (telemedicine data included in a patient's medical record); COLO. REV. STAT. § 25-1-801(d)(4) (2007) (telemedicine data included in a patient's medical record); OKLA. STAT. tit. 36, § 6804 (2008) (requiring providers to give telemedicine patients: "A statement that patient access to all medical information transmitted during a telemedicine interaction is guaranteed, and that copies of this information are available at stated costs, which shall not exceed the direct cost of providing the copies . . .").

services,[142] or provide specific timetables for insurers.[143] On the other hand, at least one state has repealed pre-HIPAA legislation limiting consumer access to avoid conflict with the Privacy Rule.[144]

Some states regulate the disclosure of particular types of health information. For example, many states mandate the confidentiality of sensitive medical conditions documented in government registries of birth defects, cancer, genetic testing, chronic disease, mental health, venereal diseases, and HIV/AIDS.[145] A few states have enacted more particular or distinctive restrictions: the District of Columbia has a special statute protecting records of child abuse, Illinois protects information stored in a registry for spinal cord injuries, and Texas protects information stored in a registry of Agent Orange victims.[146]

Although HIPAA provides HHS with the authority to enforce privacy regulations through civil money penalties,[147] neither the statute nor the Privacy Rule excludes other forms of legal action under other bodies of U.S. law, and some states provide for private causes of action related to health information privacy. Under these state laws, patients may pursue civil actions against health care providers or insurers for access and disclosure violations, with a wide range of possible remedies and differing statutes of limitations.[148] California, Connecticut, Maryland, Montana, New Hampshire, Ohio, Washington, West Virginia, and Wyoming are a few states that support causes of action for a failure to

142. *See* ARIZ. REV. STAT. § 12-2291 (2008) (ambulance services).

143. Several states require that insurers respond to consumer requests to amend medical records within 30 days. *See* 215 ILL. COMP. STAT. 5/1010 (2008); ME. REV. STAT. ANN. tit. 24-A, § 2210(1) (2008); MINN. STAT. § 2A.498 (2007); N.J. STAT. ANN. § 17:23A-9 (2008); OR. REV. STAT. § 746.645 (2007); WIS. STAT. ANN. § 610.70(3)(a) (2007); OHIO REV. CODE § 3904.09 (2008); N.C. GEN. STAT. § 58-39-50 (2007); GA. CODE ANN. § 33-39-10(a)(1).

144. UTAH CODE ANN. § 78B-5-618 (2008) (bringing state law into compliance with HIPAA through its enactment in 2003, by repealing UTAH CODE ANN. § 78-25-25 (1971), which required a patient's attorney to present written and notarized authorization to a hospital before a patient could gain access to medical records).

145. *See, e.g.,* S.D. CODIFIED LAWS § 34-14-1 (2008) ("All information, interviews, reports, statements, memoranda, or other data procured by the department of health . . . for the purpose of reducing morbidity or mortality shall be strictly confidential . . . ."); *id.* § 34-22-12.1 (communicable diseases including HIV); *id.* § 34-14-22 (predictive genetic testing); *id.* § 27A-12-26 (mental health services); *id.* § 34-23-2 (venereal diseases); *id.* 34-20A-90 (alcohol and drug abuse treatment facilities).

146. D.C. CODE § 4-1302.01 (2008); 410 ILL. COMP. STAT. 515/3 (2008); TEX. HEALTH & SAFETY §§ 83.002–83.005 (2007).

147. 45 C.F.R. § 160.418 (except as otherwise provided by 42 U.S.C. § 1320d-5(b)(1); civil penalty by HHS is not exclusive).

148. For example, under California law, an individual "may bring an action against any person or entity who has negligently released confidential information or records concerning him or her . . . for either or both of the following: (1) Nominal damages of one thousand dollars . . . [and] (2) The amount of actual damages, if any, sustained by the patient." Cal. Assemb. Bill 211 § 1 (CAL. CIV. CODE § 56.36(a)).

provide access to patient records.[149] Rhode Island, among others, provides patients with the right to sue an insurer for unlawful disclosure of medical information.[150]

A few states have created additional protections and a generalized privacy right in medical records through a "patient bill of rights."[151] Most states uphold some version of physician–patient privilege in court, but a few have especially narrow constructions of the privilege or none at all.[152] Although the more general rule is that medical files belong to the health care provider that compiles or holds them,[153] New Hampshire law assigns property rights in the files to the consumers represented in those files.[154]

149. CAL. HEALTH & SAFETY CODE § 123120 (2007) (equitable relief with costs and attorneys fees); CONN. GEN. STAT. § 38a-995 (2008) (equitable relief against insurance company with costs and reasonable attorney's fees to the prevailing party); MD. CODE ANN., HEALTH-GEN. § 4-309(f) (2008) (liability for actual damages); MONT. CODE ANN. § 50-16-553 (2007) (liability for pecuniary losses and reasonable attorneys fees under a three-year statute of limitations); N.H. REV. STAT. ANN. § 151:30 (2008) (equitable relief for violation); OHIO REV. CODE ANN. § 3701.74(C) (2008) (action to enforce the patient's right of access); WASH. REV. CODE § 70.02.170 (2008) (liability for actual damages (but not consequential or incidental damages) reasonable attorneys' fees and all other expenses reasonably incurred to the prevailing party under a two-year statute of limitations); W. VA. CODE § 16-29-1(e) (2008) (attorney fees and costs, including court costs); WYO. STAT. ANN. § 35-2-616 (2008) (equitable relief plus liability for pecuniary losses sustained as a result of the violation and reasonable attorneys fees under a two-year statute of limitations).

150. R.I. GEN. LAWS § 5-37.3-4(a)(1) (2008) (providing a cause of action with actual and punitive damages for release of a patient's confidential health care information without authorization).

151. *See* MASS. GEN. LAWS ch. 214, § 1B (2008) (right of privacy and remedy to enforce); TENN. CODE ANN. § 68-11-1502 (2010) (right to privacy for care received at a health care facility); VA. CODE ANN. § 32.1-127.1:03 (2010) ("right of privacy in the content of his health records"); FLA. STAT. § 381.026(4) (2008) (Florida Patient's Bill of Rights and Responsibilities); MINN. STAT. § 144.651 (2009) (Health Care Bill of Rights).

152. *See, e.g.*, Solomon v. State Bd. of Physician Quality Assurance, 155 Md. App. 687, 703–04 (Md. Ct. Spec. App. 2003) ("[C]ommunications made to a physician in his professional capacity by a patient are neither privileged under the common law of Maryland, nor have they been made so by statute.") (quoting Butler-Tulio v. Scroggins, 774 A.2d 1209, (Md. Ct. Spec. App. 2001), *cert. denied*, 366 Md. 247, 783 A.2d 221 (2001)); Commonwealth v. Senior, 744 N.E.2d 614, 617 (Mass. 2001) (finding no statutory patient-physician testimonial privilege in Massachusetts); *see also* Whalen v. Roe, 429 U.S. 589, 602 n.28 (1977) ("The physician-patient evidentiary privilege is unknown to the common law. In States where it exists by legislative enactment, it is subject to many exceptions and to waiver for many reasons.").

153. *See, e.g.*, VA. CODE. ANN. § 32.1-127.1:03 (2008). *See generally* Steven M. Harris, *Make Sure You Own Your Patients' Medical Records*, AMNEWS, Nov. 4, 2002, http://www.ama-assn.org/amednews/2002/11/04/bica1104.htm.

154. N.H. REV. STAT. ANN. § 332-I:1 (2008) ("All medical information contained in the medical records in the possession of any health care provider shall be deemed to be the property of the patient.").

Finally, courts in a number of states have recognized common law rights and responsibilities pertaining to medical privacy,[155] including physician obligations to treat patient records in confidence.[156] At the same time, several state courts have read such rights or obligations narrowly or have repudiated them altogether.[157] For example, the Court of Special Appeals of Maryland has held that "there is no testimonial physician-patient privilege in Maryland outside of the mental health field."[158]

II. NETWORK EFFECTS IN HIT

In some industries, consumers' valuation of a product increases as others use the product as well. [159] For example, the benefit a consumer may derive from the telephone or the Internet depends on the number of others using the network.[160] In this manner, consumers of network goods fail to capture the full benefit of their consumption. Correspondingly, consumers may tend to under–consume such network goods.[161] Network effects are so–called as they have long been observed in industries dependent on physical networks, such as the telephone network.[162] In addition, they typically arise in industries, such as the computer industry, that depend on the provision of a durable good (e.g., a computer) and a complementary good or service (e.g., software).[163] In the abstract, HIT generally fits at least the second model and interoperable HIT fits the first as well.

The presence of network effects in an industry may have implications not just for individual consumer preferences, but also for development, production, and competition among producers or vendors.

155. For a general discussion of these state common law issues, see Pritts 2002, *supra* note 133, at 325, 330–32.

156. "Individuals have a right to and an expectation of privacy related to their medical information, and this right and expectation of privacy is reflected in our public policy." Coy v. Wash. County Hosp. Dist., 372 Ill. App. 3d 1077, 1083 (Ill. App. Ct. 5th Dist. 2007).

157. Pritts 2002, *supra* note 133, at 331.

158. *See* Solomon v. State Bd. of Physician Quality Assurance, 155 Md. App. 687, 703 (Md. Ct. Spec. App. 2003).

159. Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424, 424 (1985) ("There are many products for which the utility that a user derives from consumption of the good increases with the number of other agents consuming the good.").

160. *See id.*

161. *See, e.g.*, Michael L. Katz & Carl Shapiro, *Technology Adoption in the Presence of Network Externalities*, 94 J. POL. ECON. 822, 825 (1986).

162. *See, e.g.*, *id.* at 823 (citing Dennis W. Carlton & J. Mark Klamer, *The Need for Coordination Among Firms, with Special Reference to Network Industries*, 50 U. CHI. L. REV. 446 (1983) and others).

163. *Id.*

For example, network effects may be associated with excess inertia, path dependence, or a tendency toward monopoly in certain industries. Network effects are not necessarily barriers or impediments to competition. Still, with such goods (or in such industries), there may be special significance to consumer expectations (about, e.g., future development and consumption),[164] and there may be a bias towards underinvestment, as consumers anticipate failing to capture the full benefits of their own consumption.[165] In addition, where products (or networks) offered by different firms are incompatible with each other, "the firms' joint incentives for product compatibility are lower than the social benefits."[166] Network effects may bear on product development and introduction[167] and pricing[168] as well.

Network effects associated with HIT adoption thus may raise various policy issues, as HIT appears to exhibit characteristics of network industries.[169] For example, as noted in a recent CBO Report, "Providers who can perform functions electronically (such as communicating with each other, sending and receiving medical records, prescribing medications electronically, and ordering laboratory and imaging procedures) gain when other providers develop similar [compatible or interoperable] electronic capabilities."[170] Further, there is some empirical evidence that HIT is subject to network effects. Specifically, Miller and Tucker have observed local network effects in HIT adoption, finding a robust and positive relationship between the installed base of hospital HIT in a given local health service area and the likelihood of adoption by additional hospitals.[171] That is, generally, the more hospital HIT there is in a

164. Michael L. Katz & Carl Shapiro, *Product Introduction with Network Externalities*, 40 J. INDUS. ECON. 55, 74 (1992).

165. *See generally, e.g.*, Katz & Carl, *supra* note 159.

166. *Id.* at 425. At the same time, firms may have too much incentive to agree on compatibility if it will increase the costs of production. *See* Michael L. Katz & Carl Shapiro, *Product Compatibility Choice in a Market with Technological Progress*, 38 OXFORD ECON. PAPERS 146 (1986).

167. *See, e.g.*, Katz & Shapiro, *supra* note 164; Jay Pil Choi, *Irreversible Choice of Uncertain Technologies with Network Externalities*, 25 RAND J. ECON. 382 (1994); Eirik G. Kristiansen, *R&D in the Presence of Network Externalities: Timing and Compatibility*, 29 RAND J. ECON. 531 (1998).

168. Kristiansen, *supra* note 167; *cf.* Nicholas Economides, *Desirability of Compatibility in the Absence of Network Externalities*, 79 AM. ECON. REV. 1165, 1165–66 (1989) (stating that equilibrium prices and profits tend to be higher with compatibility, even ruling out "positive consumption externalities . . . that would naturally lead to similar conclusions").

169. *See* Miller & Tucker, *supra* note 12, at 21 (estimating the average network effect in states without strong state privacy laws, in addition to federal laws, to be about 6%).

170. CONG. BUDGET OFFICE, *supra* note 10, at 20.

171. Miller, *supra* note 21, at 231 (estimating the network effect in states without strong privacy laws to be about 6%).

service area, the more likely it is that additional hospitals in the area will adopt HIT.[172]

These network effects, however, are contingent on the extent of privacy regulation in a given state. In fact, these effects are observed to disappear entirely in states that apply certain consent requirements to hospitals.[173] In addition, because they tend to suppress the local network benefits associated with hospital eHR adoption, these state laws are associated with lower rates—up to 25% lower—of HIT adoption.[174] The data also suggest that hospitals adopting eMRs in states with privacy protections are more likely to adopt proprietary, closed systems than open or interoperable ones.[175] Network effects in HIT, therefore, raise a balancing issue, as certain state law privacy provisions appear to suppress network benefits associated with HIT adoption but may serve other social interests.

Standard setting issues also may be implicated in such network industries. Standard setting—private, public, or some public/private hybrid—can be pro–competitive under a wide variety of circumstances, perhaps ameliorating coordination problems in network industries.[176] In HIT, such coordination problems may be addressed by standards covering physical qualities of hardware, architectural or formatting aspects of applications or systems, or substantive policy commitments for information handling.[177]

---

172. *See id.* As explained below, this effect is observed across states that have not adopted certain privacy regulations, pertaining to hospital sharing of health information, above the federal floor established by HIPAA, the federal Privacy Rule, and other federal laws. Also explained below is that this positive network effect essentially disappears in states that have adopted such hospital health privacy laws above the federal floor.

173. Miller, *supra* note 21, at 231. Most of the data presented by Miller was collected prior to HHS' adoption of the Privacy Rule, so absent state law, there were no privacy laws applying to hospitals.

174. Miller & Tucker, *supra* note 12, at 1; Miller, *supra* note 21, at 231.

175. Miller, *supra* note 21, at 232.

176. For example, standard setting can help to "avoid many of the costs and delays of a standards war," in which substitute but incompatible products seek to become dominant, or a *de facto* standard. DEP'T OF JUSTICE & F.T.C., ANTITRUST ENFORCEMENT AND INTELLECTUAL PROPERTY RIGHTS: PROMOTING INNOVATION AND COMPETITION 34–35 (2007), *available at* http://www.ftc.gov/reports/innovation/P040101PromotingInnovationandCompetitionrpt0704.pdf (recognizing potential benefits of standard setting, while noting possible competitive concerns, such as manipulation of the standard-setting process). It has also been observed that standard setting can clear "patent thickets" that may impede the development of follow-on products, especially in certain IT industries. *See* F.T.C., TO PROMOTE INNOVATION: THE PROPER BALANCE OF COMPETITION AND PATENT LAW AND POLICY 152 (Oct. 2003), *available at* http://www.ftc.gov/os/2003/10/innovationrpt.pdf.

177. *See, e.g.*, Carr, *supra* note 81, at 181–82; Dente, *supra* note 50, at 278; Ferguson, *supra* note 25, at 140; Kolodner, *supra* note 34, at 267–68; Tony Trenkle, Dir., Office of E-Health Standards & Servs. at the Centers for Medicare & Medicaid Servs., Dep't of Health & Human Services, Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 282–83 (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/

In fact, many stakeholders have identified a lack of standards as a barrier to HIT adoption;[178] not incidentally, various standard-setting efforts are underway. Although many standards are voluntary, others—such as CMS standards for eRx promulgated under the Medicare Modernization Act[179]—have the force of law.[180] HHS also has helped foster certification standards and processes for HIT products.[181] HHS involvement in standard setting continues under the Recovery Act. For example, the Act establishes an HIT Standards Committee "to recommend to the National Coordinator standards, implementation specification, and certification criteria for the electronic exchange and use of health information for the purposes of adoption" of nationally recognized standards for HIT.[182] ARRA standard setting is underway. In January 2010, CMS published a notice of proposed rulemaking (NPRM) to define the "meaningful use" of eHR technology and provide incentive

healthcare/hcd/docs/hcdwksptranscript.pdf). *But cf.* Letter from Stephen Downs, Robert Wood Johnson Found., David Lansky, Markle Found., JP Little, RxHub, Steve Shihadeh, Microsoft & Myrl Weinberg, Nat'l Health Council, to Hon. Michael O. Leavitt, Sec'y, Dep't of Health & Human Servs., and Chairman, A.H.I.C., Dissenting Statement on PHR Certification Process (Mar. 13, 2007) (on file with author) (suggesting that the certification process for PHRs would likely stifle innovation and that these risks outweigh the benefits); David C. Kibbe & Curtis P. McLaughlin, *The Alternative Route: Hanging Out the Unmentionables for Better Decision Making in Health Information Technology*, HEALTH AFF. w396, w396 (2008), *available at* http://content.healthaffairs.org/cgi/reprint/hlthaff.27.5.w396v1 ("[R]elying on established industry experts has left us with a standards process that is complex and burdened by diverse goals, easy for entrenched interests to dominate, and reluctant to deal with potentially disruptive technologies.").

178. *See* Ferguson, *supra* note 25, at 139 ("[I]nteroperability is certainly a requirement to make HIT go.").

179. *See* 42 C.F.R. § 423.160 (standards for electronic prescribing); *see also* Trenkle, *supra* note 177, at 283.

180. In addition, under the 2006 Executive Order, "As each agency implements, acquires, or upgrades health information technology systems used for the direct exchange of health information between agencies and with non-Federal entities, it shall utilize, where available, health information technology systems and products that meet recognized interoperability standards." Exec. Order No. 13,410, 71 Fed. Reg. 51,089 (Aug. 28, 2006) [hereinafter 2006 Exec. Order]. Such interoperability standards are those recognized as such by the Secretary of HHS. *Id.*

181. *See, e.g.*, Dep't of Health & Human Servs., Health IT Certification, *available at* http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&cached=true&objID=1196&PageID=15507 (last visited April 1, 2010). A list of certified products is available at http://www.cchit.org/products (last visited April 1, 2010).

182. American Recovery and Reinvestment Act of 2009 (Recovery Act), Pub. L. No. 111-5, § 3003(a), 123 Stat. 115, 238 (2009). The ONC must adopt an initial set of standards by the end of 2009. § 3004(b)(1). However, the Recovery Act will not require private entities to comply with those standards. § 3006(a). The ONC also must develop and make available to providers "qualified electronic health record technology" unless HHS determines that the marketplace is "substantially and adequately" meeting "the needs and demands" of providers. § 3007(a).

payments for the meaningful use of certified eHRs.[183] At the same time, HHS published an interim final rule and a request for comments regarding an Initial Set of Standards, Implementation Specifications, and Certification Criteria for eHRs.[184]

In some circumstances, however, standard setting can raise competition issues. As Carlton and Klamer have put the general problem, "[c]oordination among firms presents a policy dilemma. Efficiency may require coordinated action, but coordinated action can stifle competition and make collusion more likely."[185] Excessive standard setting may constrain innovation, just as appropriate standard setting may further it. Where products are incompatible, "a government agency that has the authority to impose one of the products as a mandatory standard may intervene to prevent inefficient stranding of earlier buyers."[186] Such standard–setting, however, may itself be socially harmful as it may induce an inefficient R&D race.[187]

Although government standard setting may speed HIT adoption by lessening coordination problems, some commentators have suggested that the emphasis on standard setting in HIT has been excessive and that excessive or premature standard setting may be counter–productive for HIT development.[188] In particular, some commentators have criticized standard setting for PHRs, arguing that it is "likely to . . . stifle innovation by prematurely locking in current approaches to PHRs and deterring new entrants in a field that is newly developing."[189]

Bracketing questions of net effects, it is important to note that HHS recognition of standards can have a tremendous impact, whether standards are required under regulation or endorsed in a less formal

183. Electronic Health Record Incentive Program, 75 Fed. Reg. 1843 (proposed Jan. 13, 2010) (to be codified at 42 C.F.R. pts. 412–13, 422, 495).

184. Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 75 Fed. Reg. 2013 (interim final rule published Jan. 13, 2010) (to be codified at 45 C.F.R. pt. 170).

185. Dennis W. Carlton & J. Mark Klamer, *The Need for Coordination Among Firms, with Special Reference to Network Industries*, 50 U. CHI. L. REV. 446 (1983).

186. Eirik G. Kristiansen, *R&D in the Presence of Network Externalities: Timing and Compatibility*, 29 RAND J. ECON. 531, 542 (1998).

187. *Id.* at 533 (citing J. Farrell & G. Saloner, *Converters, Compatibility, and the Control of Interfaces*, 40 J. INDUS. ECON. 9 (1992) (discussing that *ex post* standardization in the context of converters can give rise to inefficient incentives to produce compatible technologies)).

188. *See, e.g.*, Carol C. Diamond & Clay Shirky, *Health Information Technology: A Few Years of Magical Thinking?*, HEALTH AFF. w383, w386 (2008), *available at* http://content.healthaffairs.org/cgi/reprint/hlthaff.27.5.w383v1; *see also* Kibbe & McLaughlin, *supra* note 177. *But cf.* Kolodner et al., *supra* note 36, at w394 ("There is an approach that allows technology choices to proceed so that progress can continue as rapidly as possible without limiting future policy choices.").

189. Downs et al., *supra* note 177, at 1.

fashion.[190] In either case, policy makers should at least be aware of this second set of balancing issues in HIT.

III. PRIVACY PREFERENCES AND TRADE-OFFS

A. *Consumer Preferences for Privacy*

Many consumers are anxious about the privacy of electronic medical records, and these concerns may tend to slow HIT adoption. For example, survey data indicate that consumers avoid HIT utilities, such as PHRs, if they do not trust the privacy or data security provisions attached to those utilities.[191] The same data suggest that the privacy and data security policies that vendors adopt are important to many consumers considering the use of HIT, with the greatest percentage concerned about notification should there be unauthorized disclosure of their health information.[192] Further, consumers who worry about medical privacy may be less likely to insist that their providers adopt HIT.[193] Given these background concerns, reports of privacy or security failures can undermine consumer trust in HIT.[194]

In addition, consumers who are concerned about health information privacy may engage in "privacy protective behavior"—seeking to safeguard their health information by withholding information from their providers, paying out–of–pocket for covered care, or simply avoiding treatment altogether.[195] Indeed, the ARRA recognizes this risk, tasking

190. *See, e.g.*, Ferguson, *supra* note 25, at 180 (describing the great strides made in the last few years attributed to ONC standard-setting initiatives that have "fundamentally changed the marketplace").

191. MARKLE FOUND., *supra* note 86, at 3 (Westin and Knowledge Networks national survey) (indicating that 56.8% of those consumers "not interested" in PHRs cite privacy and confidentiality concerns as key); *cf.*, McGraw, *supra* note 31, at 143 (discussing that not having appropriate protections in place deepens consumer distrust and can create a "chilling effect").

192. MARKLE FOUND., *supra* note 86, at 3 (indicating that 60% of consumers say notification would be "essential," 32% "a factor," and 8% "nice").

193. *See* McGraw, *supra* note 31, at 143; *cf.* Uhrig, *supra* note 95, at 179 (suggesting that patient education will increase interest in HIT).

194. *See, e.g.*, McGraw, *supra* note 31, at 143 (stating that news of privacy failures "creates chilling effect that keeps people from trusting in these systems"); Kolodner, *supra* note 34, at 269 (discussing the importance of building trust in the privacy and security of a network); Pritts, *supra* note 86, at 289 (discussing consumer "needs for privacy and control and trust"); *cf.* Scriban, *supra* note 31, at 246 (describing various "trust decision[s]" consumers make in authorizing access to their Health Vault (PHR) records); Pritts, *supra* note 86, at 289 (discussing the difficulty for consumers to know what conduct may be covered by various bodies of law or subject to redress).

195. McGraw, *supra* note 31, at 142; Pritts, *supra* note 86, at 292 (discussing survey data from the California Health Care Foundation that indicate "approximately 8 percent of the population" engages in protective behavior in the face of inadequate safeguards); *cf.* Harris

the HIT Policy Committee with making recommendations related to "technologies that protect the privacy of health information and promote security in a qualified health record . . . with the goal of minimizing the reluctance of patients to seek care . . . because of privacy concerns."[196]

Broadly, there are two types of privacy concerns associated with personal health information. First, most consumers have a basic desire for some form of health information privacy independent of any particular risks attached to violations of that privacy. Alan Westin has termed this a " 'pure privacy' position—a sense of violation or intrusion if their sensitive health information is seen by an unknown third party, even if access is only for 'research' (no insurance or employer access is involved); even if a promise of anonymity is offered; and even if no actual harm to reputation is likely to result from such research activity."[197] Surveys conducted at Mayo Clinic suggest that, for many consumers, "their greatest concern about privacy actually had to do with their privacy locally . . . [A] neighbor . . . may still sometime be able to see [their] protected health information in the course of their work."[198]

This basic desire to shield details of our health conditions from others may be grounded in fundamental notions of liberty and autonomy.[199] As Cass Sunstein has observed, "patients, like other human beings, should have a presumptive right to control information that they consider private, simply as part of their liberty."[200] Indeed, the Supreme Court has identified certain rights to privacy protected under the due process clause of the Fourteenth Amendment to the U.S. Constitution.[201] In *Roe v.*

Interactive, *Harris Poll #27: Many U.S. Adults are Satisfied with the Use of Their Personal Health Information* (Mar. 26, 2007), http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Health-Privacy-2007-03.pdf [hereinafter *Harris Poll*] (indicating that 17% of those surveyed reported having withheld information from doctors and hospitals due to privacy concerns).

196. American Recovery and Reinvestment Act of 2009 (Recovery Act), Pub. L. No. 111-5, § 3002(b)(2)(B)(i), 123 Stat. 115, 234 (2009).

197. WESTIN, *supra* note 20, at 15.

198. Wood, *supra* note 31, at 184.

199. *See* Terry & Francis, *supra* note 11, at 698 (2007) ("The accepted rationale for health privacy and confidentiality is autonomy.") (citing TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 410 (4th ed. 1994)); *see also* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1088, 1116–17 (2002) (discussing theories of privacy rooted in personal autonomy and dignity).

200. Cass Sunstein, *Privacy and Medicine: A Comment*, 30 J. LEG. STUD. 709, 710 (2001); *see also* Mike Koetting, *Comments on Privacy and Medicine* 30 J. LEG. STUD. 703, 703–04 (2001) ("So why the great uproar about privacy? In part, people would simply prefer to keep their health concerns to themselves.").

201. *See* Whalen v. Roe, 429 U.S. 589, 599 (1977) (stating that the right to privacy is "founded in the Fourteenth Amendment's concept of personal liberty") (citing Roe v. Wade, 410 U.S. 113, 152–53 (1973)). *See also* Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 851 (1992) (stating that matters "involving the most intimate and personal choices a person

Whalen, the Court explained that the constitutionally protected "zone of privacy" includes "the individual interest in avoiding disclosure of personal matters."[202] And, although the exact scope of the protection remains ambiguous,[203] courts have held that medical information falls within this zone: "There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection."[204]

In addition to autonomy or liberty–based notions of privacy, one might also advance utilitarian—or generally consequentialist—arguments in favor of privacy protection. For example, disclosure of sensitive health information can have adverse effects on patients, ranging from embarrassment, to unemployment, or even ostracism.[205] Further, doctor-patient confidentiality creates incentives for patients to reveal pertinent information about their conditions—for some patients, it is a threshold requirement if they are to seek medical care at all.[206]

Bracketing the diminishing marginal utility of wealth, patients are likely to weigh tangible harms associated with invasions of privacy in a

---

may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment").

202. *Whalen*, 429 U.S. at 598–99.

203. In *Whalen*, the Court upheld a New York law requiring doctors to provide the state a copy of all prescriptions written for certain drugs with both illegal and legal uses. The court observed that these disclosures are not "meaningfully distinguishable from a host of other unpleasant invasions of privacy that are associated with many facets of health care." *Id*. at 601. It continued: "[D]isclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient." *Id*. As the Third Circuit recently explained in *Citizens for Health v. Leavitt*, "the question of the scope of the constitutional right to privacy in one's medical information is largely unresolved." 428 F.3d 167, 178 n.10 (3rd Cir. 2005). *See also* Hill v. Colo., 530 U.S. 703, 717 n.24 (2000) (finding the common-law privacy "right" to be left alone "is more accurately characterized as an 'interest' that States can choose to protect in certain situations") (citing Katz v. United States, 389 U.S. 347, 350–51 (1967)).

204. United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3rd Cir. 1980). *See also* Solove, *supra* note 199, at 1107 n.93 (collecting cases). Note, too, that state common law generally recognizes a private cause of action sounding in torts for invasions of privacy. *See* Restatement (Second) of Torts § 652 (1965).

205. *See* Sunstein, *supra* note 200, at 711; Norman M. Bradburn, *Medical Privacy and Research*, 30 J. LEG. STUD. 687, 691 (2001). We do not contend that any particular privacy protective regime falls out of a utilitarian analysis. In fact, the importance of further study of the positive and negative effects of various regulatory regimes is one of the policy emphases of this Article. In the interim, we suspect that many utilitarian analyses ought to be regarded as indeterminate. We note simply that utilitarian arguments have been advanced on behalf of health information privacy and that there are utilitarian grounds that may be considered.

206. *See* Sunstein, *supra* note 200, at 711; Terry & Francis, *supra* note 11, at 699. Some who view privacy as a fundamental right, however, chide this instrumentalist approach to privacy, fearing that it provides a slippery slope to allowing privacy concerns too easily to give way to competing values, such as the lower healthcare costs and reduced medical errors that HIT promises. *See id*.

roughly homogenous fashion—a dollar lost is a dollar lost. On the other hand, the degree to which patients demand privacy for its own sake is likely to vary substantially.[207] Indeed, a relatively large amount of survey and experimental data indicates that consumers have heterogeneous privacy preferences.[208] For example, a Medicare recipient may be more reluctant to share personal information than a twenty–year-old college student who maintains a Facebook page and "tweets" regularly about her daily life.[209] On the other hand, an older person who suffers from multiple ailments, sees multiple treating physicians, and on occasion requires critical care may have very different views about trade–offs between the medically optimal flow of health information and extremely rigorous privacy protections than, say, a typical person in her twenties, for whom chronic illness, co-morbidities, and complex teams of health care providers may be distant abstractions.

The second type of concern regards the tangible damage that can result when one person uses another's personal health information to commit fraud. Medical records typically contain sensitive personally identifying information, such as some combination of patients' names, addresses, and social security numbers. A thief could use such information to access victims' existing credit card, checking, savings, or other accounts, or to create new accounts in the victims' names.[210] Because medical records also have information about health insurance, and health

207. As Daniel J. Solove observes, "Because privacy involves protecting against a plurality of different harms or problems, the value of privacy is different depending upon which particular problem or harm is being protected. Not all privacy problems are equal; some are more harmful than others. Therefore, we cannot ascribe an abstract value to privacy. Its value will differ substantially depending upon the kind of problem or harm we are safeguarding against." *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 763 (2007).

208. For example Alan Westin has found evidence that consumers can be grouped into three categories based on their views on privacy: privacy fundamentalists; privacy pragmatists; and privacy unconcerned. *Opinion Surveys: What Consumers Have to Say About Information Privacy: Hearing Before the Subcomm. on Commerce, Trade and Consumer Protection of the Comm. on Energy and Commerce*, 107th Cong. 18 (2001) (statement of Alan Westin, Professor Emeritus, Columbia University) *available at* http://archives.energycommerce.house.gov/reparchives/107/hearings/05082001Hearing209/Westin309.htm [hereinafter Westin, *Opinion Surveys*]. *See also* Il-Horn Hann et al., *Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach*, 24 J. MGMT. INFO. SYS. 13 (2007); Sarah Spiekermann et al., *E-privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior* (2001), http://www.ischool.berkeley.edu/~jensg/research/paper/grossklags_e-Privacy.pdf; Bernardo A. Huberman et al., *Valuating Privacy*, http://infosecon.net/workshop/pdf/7.pdf.

209. Trenkle, *supra* note 177, at 282 ("[P]rivacy and security . . . mean different things to different people . . . The 75-year-old on Medicare has a very different idea of privacy and security than the 18-year-old who is text messaging and doing a lot of things on the web today."); *see also*, Pritts, *supra* note 86, at 307 ("People have . . . a wide range of privacy thresholds that they are comfortable with.").

210. *See* SYNOVATE 2006 REPORT, *supra* note 17, at 17.

information, consumers also may be subject to "medical identity theft," which the FTC has defined as the use of "your personal information without your knowledge or consent to obtain, or receive payment for, medical treatment, services, or goods."[211]

Recent data find that 8.1 million Americans (3.6% of the adult population) reported becoming aware that they were a victim of some sort of identity fraud in 2007.[212] There are two basic varieties of identity fraud: existing account and new account. Existing account fraud involves the use of the victim's account information, such as a credit card number, along with other personally identifying information to make unauthorized charges on the victim's existing account. New account fraud is more akin to what commonly may be thought of as identity theft: a thief uses the victim's personal information, such as social security number, date of birth, and address, to set up new accounts (e.g., credit cards, cell phones) under the victim's name. Because new account fraud can be difficult to detect and rectify, it is much more costly to consumers and businesses than existing account fraud.[213] New account fraud also is less common than existing account fraud due to the larger costs involved in setting up a false identity.[214] For 2006, the FTC reported that 78% of all identity theft reported involved misuse of existing accounts.[215]

In most cases, victims of identity fraud do not know how the thief obtained their personal data.[216] Of those who do know, however, most

211. F.T.C., RESOLVING SPECIFIC IDENTITY THEFT PROBLEMS, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html#MedicalIdentityTheft. The Commission's Bureau of Consumer Protection maintains an Identity Theft web page, with information for consumers, businesses, law enforcement, and others, at http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html. This definition would seem to include medical purchases made with credit cards, which would not be related to HIT.

212. JAVELIN STRATEGY & RESEARCH, 2008 IDENTITY FRAUD SURVEY REPORT: CONSUMER VERSION 4 (Feb. 2008) [hereinafter JAVELIN 2008 REPORT]. An FTC/Synovate survey conducted in 2006 estimated that 8.4 million Americans (or 3.7% of the adult population) were identity theft victims. *See* SYNOVATE 2006 REPORT, *supra* note 17, at 4.

213. *See* GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 8 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf [hereinafter GAO 2007 REPORT]. For example, the FTC reports that the median value of goods and services obtained by identity thieves was $457 for existing account fraud, compared to $1,350 for new account fraud, and that the median consumer out-of-pocket expense was $0 and four hours for existing account fraud compared to $40 and ten hours for new account fraud. *See* SYNOVATE 2006 REPORT, *supra* note 17, at 5.

214. *See* GAO 2007 REPORT, *supra* note 213, at 22 (reporting that most thieves prefer credit or debit card numbers because these can quickly be converted into cash as opposed to the more labor-intensive process of setting up a new account under a false identity).

215. *See* SYNOVATE 2006 REPORT, *supra* note 17, at 4.

216. *See* JAVELIN 2008 REPORT, *supra* note 212, at 5–6 (reporting that 65% of victims did not know how the thief gained access to their information); SYNOVATE 2006 REPORT, *supra* note 17, at 30–31 (reporting that 56% of victims did not know how the thief gained access to their information).

(79%) report that the thief obtained the data through direct contact (e.g., theft or retrieval of a lost wallet, stolen mail, or from a transaction).[217] Seventeen percent of those surveyed reported that the thief was a friend or family member, but only seven percent of known theft comes from data breaches.[218]

Medical identity theft—a type of identity fraud to which medical records may be especially susceptible—appears to be relatively rare. According to an FTC survey, three percent of those whose personal data was misused reported that the thief had used their medical insurance,[219] and 0.4% of all identity fraud victims reported that their personal data was used to create a new medical insurance policy.[220] The same survey found that three percent of victims reported that their information was used to obtain medical treatment, services, or supplies.[221] It is not clear how broad this category is, as it may cover purchases of things such as cough medicine or band aids with a stolen credit card number. Additionally, the extent to which these categories are overlapping (*i.e.*, victims report the same incidence of identity theft both as misuse of an existing medical insurance policy (or creation of a new policy) and the purchase of medical treatment, services, or supplies) is also unclear. Regardless, these figures suggest that medical identity theft is an uncommon event and that new account fraud involving medical information is even less common: from 2001 to 2005, about 0.1% of the population suffered medical insurance account misuse, and only 0.0148% of the adult population had a new medical insurance account fraudulently opened with their identity.[222]

To recognize the costs imposed by various regulatory schemes is not necessarily to impugn them—it is simply part of any regulatory cost-benefit analysis, not its conclusion. Still, maximizing consumers' net benefits should be a goal in the design of any regulatory regime. The basic fact that patients have privacy interests is clear enough; so, too, are patients' interests in effective and affordable health care. HIT systems create value in large part because they reduce the cost of communicating health information between different entities in the health care system—patients, providers, labs, hospitals, and insurers. Privacy, on the other

217. JAVELIN 2008 REPORT, *supra* note 212, at 5.

218. *Id.* at 6. The Synovate data is similar. *See* SYNOVATE 2006 REPORT, *supra* note 17, at 30.

219. SYNOVATE 2006 REPORT, *supra* note 17, at 17.

220. *Id.* at 19.

221. *Id.* at 21.

222. These calculations are based on the FTC/Synovate estimate of 3.7% of the adult population being a victim of identity fraud. Thus, .03 * .037 of the adult population suffered any form of medical identity theft and .004 * .037 of the population suffered new medical account fraud. *Id.* at 4.

hand, is at its core about limiting the flow of personal information,[223] and laws designed to protect privacy in the realm of health care do so in large part by raising the cost of collecting and sharing patients' health information. Because real world data security systems and privacy provisions are inevitably imperfect in their implementation and operation, privacy is maximally protected when there is no PHI at all. Of course, the collection and coding of PHI could be eliminated entirely if no health care were ever provided. That limiting case is more *reductio ad absurdum* than contending policy proposal. It nonetheless highlights a certain tension between information flow and information privacy. Although other laws also have the potential to impede HIT adoption,[224] it is no surprise that many have identified privacy regulation as potentially presenting the largest regulatory barrier.

It does not follow that the tradeoffs between protecting privacy and the flow of health information inevitably are simple or linear. Regulations vary in their efficiency and any given privacy provision may do more or less to promote privacy interests at greater or lesser cost. Still, given the likely tradeoffs, it is crucial to put the expected benefits and harms from loss of medical privacy into perspective.

B. *HIT and Privacy Risks*

The key privacy concern surrounding HIT appears to turn on the fact that HIT involves the storage of large amounts of personal health information in data files that may be susceptible to breach;[225] that is, some of the features of electronic information—ease of aggregation, storage, search, and transmission—that are advantageous for legitimate use of medical information may, under certain circumstances, facilitate misuse by reducing the cost of theft.[226] For example, interoperable eHRs may be subject to remote access, and large numbers of records can be stored in

223. *See* Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405 (1981) (describing one notion of privacy as "concealment of information").

224. Several Workshop panelists identified state licensure requirements as a regulatory barrier that may slow HIT implementation. *See, e.g.*, Kolodner, *supra* note 34, at 267; Wood, *supra* note 31, at 176.

225. *See, e.g.*, Pam Dixon, Exec. Dir., World Privacy Forum, Address at Federal Trade Commission Workshop on Innovations in Health Care Delivery 215–16 (April 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf); Center for Democracy & Tech., *Comprehensive Privacy and Security: Critical for Health Information Technology* 1, May 2008, http://www.cdt.org/healthprivacy/20080514HPframe.pdf (last visited Dec. 11, 2008) ("[HIT] initiatives pose heightened risks to privacy."); WESTIN, *supra* note 20, at 15.

226. *See* Terry & Francis, *supra* note 11, at 700 ("The irony is that the more inefficient a health records system, the more it is silo-based and makes interoperability difficult, the fewer confidentiality and security issues it will pose.").

something as small as a thumb drive.[227] By contrast, stealing paper records requires the presence of the thief at the point of storage and either the physical removal of the files themselves or the copying of useful information from them. As a pair of commentators assert, eMRs "are not like paper records writ larger. The differences for patient privacy and confidentiality and data security are matters of kind, not simply matters of degree."[228]

A paramount issue when assessing HIT–related risks is the extent to which a data breach—unauthorized acquisition of personal data—increases a patient's risk of becoming an identity fraud victim. Data breaches can be intentional or unintentional. For example, thieves may target personal data, either by hacking into a network remotely or by removing files from a building. Further, a thief may steal hardware (e.g., a laptop or a thumb drive) that, unbeknownst to him, contains sensitive personal information. Accidents, such as losing a laptop, or inadvertently posting personal information online, also can cause breaches. Data suggest that most breaches are due to some sort of theft or fraud[229] and that criminal use of personal data is more likely when the breach is intentional.[230] The type of data stolen also affects expected harm: social security numbers are almost always necessary to open a new account, but names and addresses alone are of little utility to fraudsters.[231] The most common type of personal data subject to breaches in 2008 was names and/or addresses (35%), followed by social security numbers

227. *See* Sharona Hoffman & Andy Podgurski, *Electronic Health Record Systems*, 22 HARV. J. L. & TECH. 104, 121 (2008) ("With a fully interoperable [HIT], EHRs could be accessed from anywhere in the country and transmitted illicitly across the world quickly, cheaply, and with little risk of detection."); Sharona Hoffman & Andy Podgurski, *Protecting Electronic Private Health Information*, 48 B.C. L. REV. 331, 335 (2007) ("Once the data is dispersed on the Internet, it becomes available to anyone who is willing to pay for it, and it cannot be expunged.").

228. Terry & Francis, *supra* note 11, at 700.

229. For example, DataLoss DB.org reports that in 2008, 67% of data breaches were due to parties outside the organization and another 8% were due to "malicious" inside acts. Further, it also reports that 53% of breaches in 2008 were due either to theft of a computer or mail, hacking, or fraud.

230. *See* GAO 2007 REPORT, *supra* note 213, at 30–31; THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN 75 n.4 (2007) *available at* http://www.ftc.gov/os/comments/healthcarewrkshp/534908-00001.pdf ("[A]s a general matter, the risk of identity theft is greater if the covered information was stolen by a thief who was targeting the data (such as a computer hacker) than if information was inadvertently left unprotected in a public location, such as in a briefcase in a hotel lobby."). *See also* Beales & Muris, *supra* note 16, at 122 (stating that risk of misuse is higher when the breach is intentional).

231. *See* Beales & Muris, *supra* note 16, at 121–22 ("Probably the most sensitive type of widely held information is social security numbers, which are crucial for opening new accounts in someone else's name" whereas "[b]reaches of information with only name and address pose virtually no consequences for consumers.").

(31%), date of birth (8%), financial information (6%), and credit card numbers (5%).[232]

According to the Open Security Foundation's Data Loss Database, there were 85 reported data breaches in the health care sector in 2009, representing 16% of all reported data breaches.[233] These affected around 4.2 million records, which represent only 2% of total records exposed.[234] Most of these breaches were intentional and were the result of thefts (36), fraud (9), or hacking (1), although the extent to which personal information rather than hardware was the target of the theft is unclear.[235] The majority of the data compromised in these breaches consisted primarily of some combination of medical records, names and addresses, and social security numbers.[236] These data suggest that breaches involving medical information are rare, but data security breach in the health care sector may increase if eHRs become more attractive targets for criminals as more providers migrate to HIT.

Although the actual incidence of harm from breach of medical records is unknown,[237] the available data suggest that the risk is relatively low. For example, two studies of intentional breaches report that new identity fraud was associated with only 0.01–0.5% of records breached.[238] These studies, moreover, likely overstate the probability of identity fraud conditional on a breach because, as discussed above, intentional thefts of personal information are associated with higher rates

232. Open Security Foundation's Data Loss Statistics, http://datalossdb.org/statistics?timeframe=last_year (last visited Mar. 19, 2010).

233. These statistics were derived from the Open Security Foundation's Data Loss Database. OPEN SECURITY FOUNDATION, CSV DATABASE (2009) http://datalossdb.org/download (follow "Download the CVS Database (with field header)" hyperlink). *See also* IDANALYTICS, NATIONAL DATA BREACH ANALYSIS 10–11 (2006) (reporting that only a small portion ofall breaches were from medical facilities), http://www.idanalytics.com/assets/whitepaper/BreachWhitePaperFinal.pdf [hereinafter IDANALYTICS 2006]. Educational institutions, businesses, and government all had higher numbers of breaches than the health care sector.

234. According to the Data Loss Database, there were approximately 220 million records exposed in 2009 as a result of data breach. OPEN SECURITY FOUNDATION, *supra* note 233. *See also* SYMANTEC, GLOBAL INTERNET SECURITY THREAT REPORT 15–16 (2008), http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf; *see also* GAO 2007 REPORT, *supra* note 213, at 18 (noting that health care facilities are responsible for only 2–3% of breached records and 7–10% of all breaches).

235. OPEN SECURITY FOUNDATION, *supra* note 233.

236. *Id*.

237. *See* OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., DEP'T. OF HEALTH & HUMAN SERVS., MEDICAL IDENTITY THEFT FINAL REPORT 3 (2009).

238. *See* IDANALYTICS, DATA BREACH HARM ANALYSIS 4 (2007) (finding misuse rates varying from 0.01% to 0.5% of files breached) ; IDANALYTICS 2006, *supra* note 233, at 25 [hereinafter IDANALYTICS 2007] (studying 4 breaches and finding a 0.098% misuse rate).

of fraud than accidental breaches.[239] Further, a survey of consumers receiving breach notification found that only two percent had suffered any kind of identity fraud.[240] After reviewing the available data and interviewing industry sources, moreover, the GAO concluded: "Comprehensive information on the outcomes of data breaches is not available . . . . but available data and information from law enforcement and industry association representatives indicated that most breaches have not resulted in detected incidents of identity theft."[241] There does not appear to be any reason to believe that the misuse rate for breached medical records is higher than that of breached records generally.[242]

Even if greater use of HIT were to increase the prevalence of breaches and/or the average size of files involved in breaches—hence the exposure of more identities[243]—increased harm would not necessarily follow. Research suggests that there may be an inverse relationship between the size of files breached and resulting identity fraud,[244] perhaps due to resource constraints that limit fraudsters' abilities to exploit the personal information they steal.[245]

This discussion has proceeded under the assumption that HIT increases privacy risks, but that is not necessarily true. Although it is likely that more information is at risk if a breach occurs in an electronic system as compared to a paper system, there are strong reasons to believe that electronic systems generally are more secure than paper records.[246] For example, encryption and strong password protection can make it harder

239. *See* IDANALYTICS 2007, *supra* note 238, at 5. *See also supra* text accompanying note 230.

240. PONEMAN INST., CONSUMERS' REPORT CARD ON DATA BREACH NOTIFICATION 5 (2008). The report does not specify whether this is new or existing account fraud.

241. *See* GAO 2007 REPORT, *supra* note 213, at 21.

242. *See id.* at 16 (reporting that a survey by the American Hospital Association of 46 hospitals found that 17 breaches from 2003 to 2007 resulted in only 6 incidences of identity fraud, usually involving only one victim).

243. In a regulatory sense, "breach" refers to improper access to the information of a single individual. For example, the FTC recently proposed " 'breach of security' as the acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual," following the definition under section 13407(f)(1) of the Recovery Act. *See* F.T.C. Notice of Proposed Rulemaking, 74 Fed. Reg. 17,914 (April 20, 2009) (to be codified at 16 C.F.R. pt. 318) (proposed rule under Recovery Act). Hence, when we speak informally of an incident of breach involving many files, we are in fact referring to an incident in which there are multiple breaches.

244. *See* IDANALYTICS 2007, *supra* note 238, at 4.

245. *See id.*; Beales & Muris, *supra* note 16, at 123.

246. *See, e.g.*, McGraw, *supra* note 31, at 143 ("[T]echnology . . . can enhance privacy, but it also magnifies the risk."); Trenkle, *supra* note 177, at 283 ("There is a lot of relation to fraud and tampering that obviously can occur with e-prescribing, but e-prescribing can also prevent a lot of that.").

to access sensitive health information stored electronically.[247] Indeed, the amount of sensitive personal information stolen from offline sources dwarfs that stolen online.[248] Further, breach detection is likely easier with electronic systems that allow automatic "red flag" auditing processes to detect anomalies in patient records.[249] Finally, as noted above, expected losses for breach fall with the size of the breach event.[250]

If expected privacy losses to consumers fall with HIT adoption, then the net benefits from privacy laws that retard HIT adoption will be overstated. That is, if HIT reduces expected consumer losses from breach (by reducing the probability of breach), then HIT and regulation are substitute instruments to protect the privacy of patients' health records. Thus, scaling back privacy regulations to reduce strictures on the electronic exchange of health information may not lead to a net reduction in privacy protection. Even if enhanced privacy protection due to the adoption of HIT does not entirely offset that lost if privacy regulations are made more lax, it must nevertheless be counted in any cost–benefit analysis.

Although the risk (or expected harm) associated with breach appears to be low for the population as a whole, we do not mean to deny the harm that might be done in any particular case. First, consumers may suffer financial account fraud; armed with a patient's social security number, name, address, and date of birth, a fraudster could set up a new account.[251] Some medical records may include bank account or credit card information from co–payments, which could be used to hijack an existing financial account. Second, patients could suffer harm related to their medical insurance policies. For example, they may find themselves bearing the expense of health care goods and services obtained without their knowledge.[252] The FTC reports that the median out–of–pocket costs

247. *See* OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., *supra* note 237, at 4 ("[M]ost of the leading experts who participated in the Town Hall agreed that, if implemented and executed properly, health IT and health information exchange could be used to prevent, detect, and help with correction of medical identity theft in a manner that has not been previously available."); *see also* Uhrig, *supra* note 95, at 166–67 ("E-prescribing is more secure, in our view, than paper."); Wood, *supra* note 31, at 184–85 (arguing that electronic systems are more secure than paper systems, particularly when combined with a strong audit system).

248. JAVELIN 2008 REPORT, *supra* note 212, at 5; SYNOVATE 2006 REPORT, *supra* note 17, at 30–31.

249. *See* OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., *supra* note 237, at 4.

250. *See supra* notes 244–245 and accompanying text.

251. *See* Beales & Muris, *supra* note 16, at 122 ("Probably the most sensitive type of widely held information is social security numbers, which are crucial for opening new accounts in someone else's name.").

252. That is, consumers may be billed for, or otherwise alleged to be responsible for, health care goods and services obtained, without their knowledge, by and for others. *See, e.g.*, PAM DIXON, WORLD PRIVACY FORUM, MEDICAL IDENTITY THEFT: THE INFORMATION CRIME

to victims of fraud on existing non–credit card accounts and new accounts (not limited to medical insurance) were $0 and $40, respectively.[253] However, in some circumstances the costs can be much higher: the 95th percentile costs of these types of fraud were $1,200 and $5,000, respectively.[254] Consumers also may encounter protracted difficulties when the contents of their medical records are altered in the course of medical identity theft.[255] Future benefits, coverage, eligibility, or even treatment issues may hinge on inaccuracies in a consumer's medical file.[256] For example, a consumer whose medical records have been corrupted as a consequence of medical identity theft may be subject to serious—perhaps fatal—errors in medical treatment or the exhaustion of her insurance coverage.[257] Given the range of possible harms to which consumers may be subject, and the potential costs of guarding against these harms, better data about the consequences of sensitive health information theft is a crucial input to ongoing policy making.

THAT CAN KILL YOU 16 (2006), *available at* http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf [hereinafter DIXON 2006]. The FTC reports that the median value of goods and services obtained by theft associated with existing non-credit card accounts and new accounts were $1,350 and $457, respectively. FTC, *supra* note 17, at 5.

253. FTC, *supra* note 17, at 5.

254. *Id.*

255. Dixon, *supra* note 225, at 216; *see also* F.T.C., *supra* note 211 (stating that inaccurate medical records can have a serious impact on the ability to obtain proper medical care and insurance benefits).

256. *See, e.g.*, United States v. Skodnek, 933 F. Supp. 1108, 1121 (D. Mass. 1996) (regarding fines and incarceration of the defendant psychiatrist convicted of making false claims to Medicare program, mail fraud, obstruction of justice, and witness intimidation).

> There is no reason to believe that this misinformation will not lead to misfortune for those whose names Skodnek used in fabricating the sessions. This is an information age. While nominally confidential, these records are vulnerable to disclosure to any number of sources. Whether it should or not, the misinformation will almost certainly have an impact on patients' lives. It may determine whether an individual will be given a health insurance policy; it may decide whether he or she will receive government clearance; it may affect a whole host of other situations.

Id. at 1121. *See also* DIXON 2006, *supra* note 252, at 5–9 (describing types of harms consumers may suffer from medical identity theft and providing examples of certain cases); AHIMA e-HIM Work Group on Medical Identity Theft, *Mitigating Medical Identity Theft*, 79 JOURNAL OF AHIMA 63, 64 (Jul. 2008) (describing an anecdote from one case of medical identity theft in which a victim was threatened with the loss of her children because her medical records included a positive test for methamphetamines for a newborn baby, which was not hers).

257. *See,* Dixon, *supra* note 225, at 216; Sharona Hoffman & Andy Podgurski, *Protecting Electronic Private Health Information*, 48 B.C. L. REV. 331, 335 (2007) ("Loss or corruption of health data can also require the duplication of painful medical tests or even cause serious and life-threatening medical errors.").

C. *Costs and Benefits of Various Privacy Regulations*

Privacy regulation takes three primary forms: consent requirements, breach notification requirements, and data security requirements. As discussed below, each type of regulation is likely to be associated with distinct costs and benefits to patients and providers. These differences may, in turn, have varying effects on HIT adoption. Consequently, the optimal *level* of privacy regulation is likely to vary across *types* of privacy regulations.

1. Consent and Authorization

Federal and state consent requirements are various. Some state privacy laws require express consent or written authorization for disclosures that are excluded from HIPAA authorization requirements, such as those made for treatment and payment purposes.[258] Because HIPAA sets a federal floor for disclosure requirements, some covered entities may adopt policies to obtain and document consent for disclosures under circumstances in which federal law would not require it.[259]

Due to the nature of the communications to which they typically apply, however, consent requirements are likely to have only a modest impact on the risk of medical identity theft or other tangible harms that may be associated with the disclosure of sensitive health information. Because breach is in most cases due to theft or fraud, and because breach due to theft or fraud is most likely to lead to tangible harm, it seems unlikely that express consent or authorization requirements—providing patients with a veto right with respect to voluntary communication between, e.g., providers, hospitals, insurers, and pharmacies—would appreciably reduce the frequency of identity theft. The benefits from consent requirements, therefore, are likely to accrue primarily in the form of "pure privacy" protection. Consent requirements, by mandating that covered entities consult with a patient before sharing the patient's health records (or the PHI within), provide patients a modicum of control over third–party access to their sensitive health information in the regular course of business.

At the same time, consent requirements perhaps most clearly impact potential HIT benefits by increasing the marginal cost of communication.

---

258. LINDA L. DIMITROPOULOS, PRIVACY AND SECUIRTY SOLUTIONS FOR INTEROPERABLE HEALTH INFORMATION EXCHANGE: ASSESSMENT OF VARIATION AND ANALYSIS OF SOLUTIONS 3-1 to 3-3 (2007) "Although the Privacy Rule allows the disclosure of health information for treatment, payment, or health care operations without consent, many state laws require such written consent to disclose health information for these purposes, using various terms in addition to *consent*, such as *permission*, *authorization*, or *release* (here, collectively referred to as *consent." Id.* at 3-2.

259. *See* NATIONWIDE SUMM., *supra* note 13, at 6–8.

For example, HIT can reduce the cost of transmitting test results between a hospital and an outside laboratory, which can improve outcomes and reduce costs by, for example, eliminating the need for duplicative tests. Requiring the hospital and the laboratory independently to obtain and document the patient's consent before transmitting results, however, reduces one of HIT's key benefits—rapid and low–cost exchange of health information. That adds cost to transactions likely to occur in any event (a hospital's access to a certain test known to be important, recent, and available), but it also adds cost to the search for, retrieval, and verification of potentially pertinent clinical information. When information search is costly, less of it is likely to get done. Recall, for example, the millions of adverse events attributable to avoidable medication errors.[260] Generally, these are deemed avoidable because they are predicated on information that is in error at the point of care, not on information that is wrong or unavailable throughout the health care system. Indeed, many errors are avoidable precisely because they involve information transmission errors.[261] Hence, at the margin, such requirements can add to health care costs *and* impede the flow of important health care information. Although HIPAA generally exempts communications like these from its authorization requirements, some state regulations do not.[262] Further, as discussed below, when state law is unclear, providers rationally may err on the side of caution—requiring unneeded documentation before disclosing health information to a third party or sometimes withholding the information altogether.

If consent requirements reduce HIT benefits, providers also will be less likely to adopt HIT in the first place. Some empirical evidence supports this hypothesis. Specifically, as discussed in Part III of this Article, eHR adoption exhibits local networks effects; hospital adoption rates tend to be a positive function of the number of hospitals in an area that have adopted eHR systems.[263] These network effects, however, disappear entirely in states that apply certain consent requirements to hospitals.[264] In addition, because they tend to suppress the local network benefits associated with hospital eHR adoption, these state laws are associated with

260. *See supra* notes 7, 57–61, and accompanying text.

261. *See* BD. ON HEALTH CARE SERVS., *supra* note 7, at 121–22.

262. *See, e.g.*, ALA. CODE § 27-21A-25 (West 2009) (requiring an HMO to obtain patient consent before releasing any information on diagnosis, treatment, or health to anyone); MASS. GEN. LAWS. ANN. 111 § 70E (West 2010) (requiring hospitals to obtain patient consent before releasing records); MINN. STAT. ANN. § 144.651 subd. 16 (requiring hospitals to obtain patient consent before releasing information).

263. *See supra* notes 169, 171–175, and accompanying text.

264. *See supra* note 169 and accompanying text.

lower—up to 25% lower—rates of HIT adoption.[265] The data also suggest that hospitals adopting eMRs in states with such privacy requirements are more likely to adopt proprietary, closed systems than open or interoperable ones.[266] In related research, Miller and Tucker analyze the effects of HIT adoption on neonatal mortality, and find that certain HIT adoption reduces infant mortality by about one percent, with gains twice as large for African American children as for whites.[267] Taken together with their research on the effect of state privacy laws on HIT adoption, it appears that various state privacy regulations that apply above the federal floor may have costs in terms of patient outcomes.[268]

2. Breach Notification

Breach notification rules generally require covered entities to notify patients when unauthorized persons gain access to the patients' PHI. These laws can reduce the expected damages from identity theft—medical or otherwise—through three primary channels. First, when a patient is informed of a breach of which she would otherwise be unaware, she can take prophylactic actions against the misuse of her information.[269] Second, if a breach has already resulted in identity theft, notification may allow a victim to limit her damages by, for example, notifying creditors or insurers and cancelling accounts.[270] Survey data suggest that consumers who learn of fraudulent activity on their accounts early are able to mitigate their financial harm.[271] Finally, breach notification requirements can create incentives for firms to take steps to prevent breach before it occurs.[272] Reputational incentives, among others, are likely to drive precautionary measures against breach. Briefly, in various ways, some *ex ante* data security measures may simply be less costly to the covered entities themselves than *ex post* notification of breaches that the measures would prevent.

265. Amalia R. Miller & Catherine Tucker, *Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records* 1 (NET INST. WORKING PAPER NO. 07-16 (2008)), *available at* http://www.netinst.org/Miller-Tucker_07-16.pdf (discussing the differential effects of state law medical privacy regimes on hospitals' adoption of HIT); Miller, *supra* note 21, at 231.

266. Miller, *supra* note 21, at 232.

267. *Id.* at 233.

268. Miller and Tucker happened to have focused on neonatal mortality, but a broader inquiry into health effects certainly could be valuable.

269. Consumers may, e.g., request new credit or insurance cards, or sign up for account monitoring services.

270. It may not be as easy for insurers to issue new account information as it is for banks. *See* OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., DEP'T. OF HEALTH & HUMAN SERVS., MEDICAL IDENTITY THEFT FINAL REPORT 21–22 (2009).

271. *See* SYNOVATE 2006 REPORT, *supra* note 17, at 57.

272. GAO 2007 REPORT, *supra* note 213, at 32.

Breach notification requirements also provide consumers with information about the security of their personal information. According to some commentators, consumers have a basic right to privacy that includes being informed when their personal information has been compromised.[273] Without settling the question of the scope of consumers' privacy rights—grounded in their constitutional rights or otherwise—we can at least recognize a potential interest in notification.

The efficacy of various breach notification requirements is unclear, however. Although survey data suggest that firms recognize the reputational costs of publicized breaches,[274] available (limited) empirical evidence does not show a relationship between state breach notification laws and the incidence of victim-reported identity fraud from 2002–2007.[275] Further, many consumers do not appear to take action in response to notification, perhaps due to the relatively low expected damages from breach.[276] As discussed above, only a very small amount of personal information is subject to security breach—the available data suggest that thieves are likely to use at most .5% of all breached records to commit fraud.[277]

Although they do not impact communication costs in the same direct manner as consent requirements, breach notification requirements also have the potential to impede HIT adoption. First, notification is costly: the average direct and indirect cost of breach events in 2008 was $6.7 million, or $202 per record breached overall and $282 per record breached in the health care sector.[278] Because some electronic databases contain more records than paper–based systems, the cost of notification per event may be higher with HIT. If the potential for breach were the same with paper–based systems and electronic ones, then entities adopting HIT would likely incur larger notification costs than those that did not. These costs may affect providers' marginal incentives to adopt (or

273. *Id.* at 33.

274. *See* PONEMAN INST., CONSUMERS' REPORT CARD ON DATA BREACH NOTIFICATION 8 (2008) (finding that abnormal customer churn is the largest cost to data breach).

275. Sasha Romanosky et al., Do Data Breach Disclosure Laws Reduce Identity Theft? (Sept. 16, 2008) (unpublished manuscript presented at the Seventh Workshop on the Economics of Information Security, Center for Digital Strategies), *available* at http://ssrn.com/sol3/papers.cfm?abstract_id=1268926.

276. The FTC reports that 44% of people who received breach notification did nothing. SYNOVATE 2006 REPORT, *supra* note 17, at 57.

277. *See* IDANALYTICS 2007, *supra* note 238, at 2.

278. *See* PONEMAN INST., FOURTH ANNUAL U.S. COST OF DATA BREACH STUDY 2, 6 (2009). Direct costs are those associated with detecting breaches and notifying customers. Indirect costs are those associated with lost business due to negative publicity from the breach. *Id*. As noted above, whereas here we refer to an event as encompassing an underlying set of facts in which one or many records may be breached, there is a regulatory sense in which an instance of breach is counted as the breach of a single individual's record. *See supra* note 243.

expand current use) of HIT, which would reduce both stand–alone and network benefits available to patients. Further, if expected costs from breach notification requirements are high, some PHR vendors may decide against entry in the first place, which is likely to have implications for competition and consumer choice.

Also, over–warning is possible here, as it is elsewhere in health care. In particular, breach notification that is unrelated to actual risk of harm could over–deter the use and adoption of HIT. There already appears to be a baseline of wariness about the security of HIT systems, and a sharp increase in breach notification could serve unnecessarily to exacerbate this concern. For example, if notifications become commonplace, consumers may begin to develop unfounded fears of HIT. Further, because maliciously-used personal data are stolen primarily from offline sources rather than online databases, substitution of paper records for electronic records may have the unintended consequence of increasing identity theft. As noted above, to the extent that consumers are over–warned, they may—at some risk to their health—engage in excess privacy–protective behavior in their interactions with health care providers.[279] Consumers may also take prophylactic steps like requesting new insurance cards, placing fraud alerts on accounts, or even cancelling accounts, which may not be justified by the risk of identity theft due to breach. In addition, fearful of incurring the direct and reputational costs of breach notification, entities that maintain confidential health records may adopt security measures that increase the cost of exchanging health information.[280]

3. Data Security Requirements

As discussed in part II of this Article, in some circumstances the FTC can bring enforcement actions against entities that fail to provide adequate safeguards for their consumers' sensitive data. Further, HHS has jurisdiction to enforce the Security Rule under HIPAA, which requires covered entities to take certain steps to protect PHI stored in electronic form.[281] Clearly, enhanced security is likely to reduce the incidence of breach and concomitant harms. If firms have sufficient private incentives to keep data secure, however, these laws may lead to over–investment in security. Indeed, some of these requirements may be superfluous. Event studies indicate that publicly traded firms suffer substantial losses when breaches occur. Although these studies do not

279. *See supra* notes 195–196 and accompanying text.

280. *See* NATIONWIDE SUMM., *supra* note 13, at 6-21 (noting that fear of liability under HIPAA has lead to restrictive policies on sharing information); GAO 2007 REPORT, *supra* note 213, at 35.

281. *See* 45 C.F.R. § 164.534 (2010).

include data from not–for–profit or privately-held entities, which characterize much of the health care industry, there is no reason to suspect that they do not suffer financial losses from breach as well. Additionally, FTC survey data suggest that firms suffer far greater financial harms from identity fraud than consumers, and even not–for–profit health care providers have incentives to minimize costs.[282] Thus, providers, hospitals, and insurers all likely have private incentives to invest in data security, although the degree to which these incentives promote the socially desirable level of security measures is unclear.

To the extent that data security rules require technical protocols—such as encryption—they affect fixed rather than marginal costs of using HIT, and moreover, may be relatively inexpensive to implement.[283] As one FTC panelist put it, with regard to engineering HIT systems from the ground up, a single privacy regime—even a stringent one—would be relatively unproblematic: "What gets expensive is . . . 50 different states change the standards as well as 14 countries and the next thing you know, it takes millions and millions of dollars worth of IT resources to rebuild these systems."[284] In some instances, however, security requirements can affect marginal costs of communicating health information. For example, covered entities may be reluctant to engage in electronic exchanges of health information if they are uncertain that others on the network have security measures that will meet the applicable legal standard.[285]

4. Legal Uncertainty

With all three types of regulation discussed above, uncertainty about prevailing legal standards also may increase the cost of health information exchange. For example, despite the range of unauthorized disclosures permitted under the Privacy Rule,

282. For example, the median value of goods and services for all categories of identity theft was $500 compared to zero for consumers. Further, the median value for new account fraud was $1,350 for firms compared to $40 for consumers. *See* SYNOVATE 2006 REPORT, *supra* note 17, at 6.

283. *See, e.g.*, HIPAA Security Rule, 45 C.F.R. § 164.312(a) (2010).

284. Dente, *supra* note 50, at 280; *see also* Berg, *supra* note 31, at 253–54 (comparing the relative ease of meeting strict state standards for Marshfield Clinic, which operates wholly within Wisconsin, with that of, e.g., GE or Epic or Cerner, who are "developing for 50 states and territories in foreign countries"). We address the issue of state law variation in Part VI.

285. *See* NATIONWIDE SUMM., *supra* note 13, at 6-25 ("Sharing personal health information among institutions requires a significant degree of trust in the technology, and in the other organizations' ability to implement it. State teams found that providers were worried that entities receiving their data might not have robust security measures (as robust as the providers' measures), and that this difference might expose them to liability in case of a security breach.").

> [M]any providers and other covered entities require patient permission to disclose personal health information for treatment, payment, and health care operations to satisfy professional ethical requirements or for risk management . . . . [M]ost stakeholder organizations . . . required patient permission for treatment purposes, even if federal or state laws did not require such permission . . . Although variation in the requirement for and content of patient permission to disclose is due largely to state law and organizational practices, "HIPAA" is often cited as the basis for requiring patients' permission for treatment.[286]

When relevant state and federal privacy regulations are not clear, parties may over–comply to avoid liability.[287] For example, ambiguous state law provisions regarding the circumstances that trigger breach notification requirements can lead to over–notification.[288] Further, unclear consent (or documentation of consent) requirements have led to substantial variation in the form and content of authorization across providers.[289] That variation, in turn, has made some providers unwilling to accept consent obtained by others.[290] Vagueness in "minimum necessary" disclosure requirements under the Privacy Rule also seems to have had a chilling effect on electronic information exchange.[291] For example, because it often is technically impossible to segregate data fields in eHRs, many hospitals allow third–party payers to have access only to paper records.[292]

Note that Miller finds a one–time *increase* in HIT adoption associated with HHS' adoption of the HIPAA Privacy Rule.[293] That is

286. NATIONWIDE SUMM., *supra* note 13, at 6-11. *See also* Dimitropoulos & Rizk, *supra* note 14, at 429 (discussing how broad variation exists in the "need for . . . and the actual process of obtaining appropriate patient consent" in the context of identifying gaps and conflicts among state laws).

287. *See* STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 224–29 (2004). Of course, the countervailing consideration for breach notification is that breach notification appears to lead to a lot of customer churn. The size of this consideration may militate toward erring on the side of not sending notification.

288. *See* GAO 2007 REPORT, *supra* note 213, at 35.

289. *See* NATIONWIDE SUMM., *supra* note 13, at 6-3 (explaining that laws that are "silent with respect to certain aspects health information exchange" can lead to varied customs, which can hinder HIT).

290. *Id.* at 6-8 ("The lack of a standard permission form, even within a state, results in different health care entities' developing their own permission form requirements and refusing to honor permissions obtained by other entities, thereby interfering with the legitimate flow of information.").

291. The Privacy Rule requires that "a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." 45 C.F.R. § 164.502(b)(1) (2010).

292. NATIONWIDE SUMM., *supra* note 13, at 6-16.

293. Miller, *supra* note 21, at 252.

interesting but not paradoxical. Certainly, the promulgation of the federal Privacy Rule did not reduce the regulatory obligations of health care providers. At the same time, for some providers, it may have lowered the perceived cost of HIT adoption precisely because it decreased providers' legal uncertainty and exposure to liability.[294]

III. STRIKING THE BALANCE

Although consumers demand privacy, it is not free. Privacy requirements can have positive effects on HIT adoption by helping to assuage consumers' concerns that their sensitive health information is secure, but beyond some threshold, it is important for policy makers to recognize that tradeoffs between privacy protection and HIT development, adoption, and use are likely inevitable. As one commenter has put it, the debate over privacy in health care should focus on "how much [privacy] we want to afford, which in turn is linked to thinking more carefully about losses from its breach."[295] Certain forms of privacy regulation appear to impose relatively large costs on eMR use while conferring relatively little in the way of tangible countervailing benefits. Of course, some may object to such balancing.[296] For example, Solove suggests that individual rights typically give way when pitted against the "common good."[297] That may be a legitimate matter of more general concern, but it does not answer critical policy and legal questions, such as the level of resources that ought to be devoted to safeguarding particular rights, or the manner in which provisions protecting countervailing interests or rights ought to be balanced.

One might take the position that fundamental rights—or their exercise or protection—are never in tension, but as we have discussed, that is entirely dubious in the instant case as it is more generally. Although exploration of such matters from a policy, legal, or ethical point of view would take us well beyond the scope of this Article, we should note that, as a general matter, our Constitutional framework balances fundamental

294. *Id.* (noting that some have theorized that this was because "HIPAA promoted some adoption of EMR by making HIPAA compliance easier to demonstrate with an electronic record than with a paper record").

295. Mike Koetting, *Comments on Privacy and Medicine*, 30 J. LEGAL STUD. 703, 707 (2001).

296. *See* Terry & Francis, *supra* note 11, at 699 ("This instrumental approach becomes dangerous when applied to institutional or industrial models of care. In such models, the notion too easily falls prey to arguments that see the generation, dispersal, and processing of longitudinal patient health information primarily as a necessity to reduce overall healthcare costs and to minimize medical error.").

297. Solove, *supra* note 207, at 761 ("Society will generally win when its interest are balanced against those of the individual.").

rights, interests, privileges, and powers in no small part because it must. Even core civil liberties are not regarded as absolute. For example, under the First Amendment, content–based regulation of speech is presumptively invalid, but certain categories of speech—e.g., obscenity[298]—are subject to no protection and others—e.g., commercial speech[299]—may be subject to substantial protection, but less than that afforded political, scientific, literary, or artistic speech. Generally, content–neutral regulation of speech is subject to intermediate scrutiny and certain species of restrictions generally are permissible. As the Court has said, "[o]ur cases make clear . . . that even in a public forum the government may impose reasonable restrictions on the time, place, or manner of protected speech . . . ."[300] More generally, "[t]he First and Fourteenth Amendments have never been treated as absolutes."[301]

Speech rights and privacy rights have been variously connected. "The unwilling listener's interest in avoiding unwanted communication . . . is an aspect of the broader 'right to be let alone' that one of our wisest Justices characterized as 'the most comprehensive of rights and the right most valued . . . .'"[302] But that right, too, is subject to variable protection, afforded special protection "in the privacy of the home,"[303] but lesser protection elsewhere.[304] Similarly, the Supreme Court has on several occasions grappled with the tension between First Amendment guarantees to the press to publicize facts and the rights of citizens to keep certain facts private.[305] These cases have called on the Court to rule on "a conflict between interests of the highest order—on the one hand, the interest in the full and free dissemination of information concerning

298. "This much has been categorically settled by the Court, that obscene material is unprotected by the First Amendment." Miller v. California, 413 U.S. 15, 23 (1973) (citations omitted).

299. *See* Thompson v. W. States Med. Ctr., 535 U.S. 357, 367–68 (2002) (re-affirming the *Central Hudson* test as a framework for evaluating government restrictions on commercial speech) (citing Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557 (1980)).

300. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989). Such regulation of protected speech "must be narrowly tailored to serve the government's legitimate, content-neutral interests but . . . it need not be the least restrictive or least intrusive means of doing so." *Id.* at 798.

301. Breard v. Alexandria, 341 U.S. 622, 642 (1951).

302. Hill v. Colorado, 530 U.S. 703, 716 (2000) (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

303. *Id.* at 717.

304. "This common-law 'right' is more accurately characterized as an 'interest' that States can choose to protect in certain situations." *Id.* (citing Katz v. United States, 389 U.S. 347, 350–51 (1967)).

305. *See* Bartnicki v. Vopper, 532 U.S. 514 (2001); The Fla. Star v. B.J.F., 491 U.S. 524 (1989); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975).

public issues, and, on the other hand, the interest in individual privacy and, more specifically, in fostering free speech."[306]

Of course, in a utilitarian calculus, to the extent that most individuals highly value a given "right" or interest, their collective valuation may trump other interests.[307] Hence, citizens may willingly agree *ex ante* to limit the circumstance under which the common good may trump an individual right. That is one route to constitutionalism (and in some sense to the rule of law), and it is not unrelated to the distinction between act–based and rule–based approaches to utilitarianism. But generally, the question whether to balance competing interests does not depend on a commitment to utilitarianism or any other form of consequentialism. It also does not require the repudiation of a rights–based approach to privacy or anything else.[308]

Returning to our concrete policy concern, when designing laws to protect consumers' sensitive health information, there are two paramount questions. To what extent do those privacy laws reduce consumer harm? And, what benefits from HIT do those privacy protections impede?

In answering the first question, it is important to note as a threshold matter that the baseline level of harm from PHI breach appears small. Further, the nexus between some privacy laws applied to HIT and harms from loss of privacy is tenuous. For example, it is unclear how state privacy laws that have stringent consent requirements reduce the risk of identity fraud; there is probably little connection between consent and avoidance of identity fraud within a treatment episode. Additionally, breach notification laws do not appear to reduce the incidence of identity fraud, and although the relationship between breach and risk of identity fraud may be direct, the available data suggest that it is very slight. Indeed, the broader class of breach notification requirements does not appear to pass a cost–benefit test. The average direct cost to responding to a breach (which almost surely is passed on to consumers) is $50,[309] but the upper bound on the median expected cost from new account fraud (the most expensive type) in the event of a breach is $1.13.[310] Indeed,

306. *Bartnicki*, 532 U.S. at 518.

307. *See* Solove, *supra* note 297, at 761.

308. *See*, *e.g.*, H.L.A. Hart, *Are There Any Natural Rights?*, 64 PHIL. REV. 175, 176 (1955) ("[A]lthough . . . all men are equally entitled to be free in the sense explained, no man has an absolute or unconditional right to do or not to do any particular thing or to be treated in any particular way; coercion or restraint of action may be justified in special conditions consistently with the general principle."); *cf.* Alan Gewirth, *Are There Any Absolute Rights?*, 31 PHIL. Q. 1 (1981) (distinguishing "absolute rights" from those that may be "overridden," or justifiably infringed).

309. *See* PONEMON INST., FOURTH ANNUAL US COST OF DATA BREACH STUDY 3 (2009).

310. This figure is calculated as follows: The Synovate 2006 study reports a median loss for new accounts and other frauds of $40 and 10 hours. Using the average hourly wage rate

even for victims in the 90th percentile of harm, the expected financial loss is only $24. Thus, extant breach notification requirements generally do not appear to be a good deal for consumers.

None of the preceding discussion should suggest that consumers derive no benefit from privacy regulations or that concerns about the privacy of health information are unfounded or unimportant. As discussed already, many patients clearly place an intrinsic value on privacy; hence, regulations may provide benefits beyond those easily measured. Moreover, society may wish to subsidize the diminution of certain extreme harms.[311] On the other hand, data available from behavioral experiments suggest that consumers are willing to supply private information for relatively small amounts of money or enhanced convenience shopping online.[312] Further, several studies have found a mismatch between *ex ante* consumer responses to general questions regarding their desire for privacy protection and the actual tradeoffs they are willing to make when faced with immediate choices.[313] Although these studies were experimental in nature and generally involved personal information that may be seen as less sensitive than PHI, they again suggest that patients may be more willing to forego certain privacy protections in return for better and/or cheaper health care than survey data suggest, especially if the sacrificed protections are of limited efficacy in preventing tangible harms. And at least for some patients, at least some of the time, an interest in optimizing information flow may be critical.

With respect to the second question—the costs of privacy requirements—empirical evidence suggests that HIT adoption rates are lower in states with stringent consent requirements. Adoption rates in these states are lower because the regulations suppress network effects associated with HIT adoption.[314] Further, states with lower levels of HIT adoption appear to have higher infant mortality rates, even after controlling for possibly confounding variables.[315] To the extent that the IOM is right

from April 2009 of $18.50, this results in median costs from the most expensive type of identity fraud of $225. Data from IDAnalytics puts a range of the probability of a breached file being used in an incidence of identity fraud between 0.0001 and 0.005.

311. *See, e.g.*, RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 383–84 (6th ed. 2003) (arguing for direct regulation where injury may be very large or—on related but distinct grounds—where injuries are fatal).

312. *See* sources cited *supra* note 208.

313. *Id*.

314. *See* Miller & Tucker, *supra* note 12.

315. *See* Amalia R. Miller & Catherine Tucker, *Can Healthcare IT Save Babies?* (SSRN Working Paper Series, 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1080262#PaperDownload (describing effects of state law privacy regimes on infant mortality). Specifically, their research suggests that certain HIT adoption reduces infant mortality by about one percent, with gains that "are twice as large for reducing African American deaths

about the potential for ameliorating serious adverse events due to medication errors by adopting appropriate HIT, we must note again that millions of such adverse events are on the table.[316] Thus, by impeding the flow of health information between providers, stringent consent requirements may impose real human costs beyond their financial costs. Consent requirements also impose direct transaction costs on consumers and providers. Breach notification requirements impose expenses on firms that can impede adoption of HIT by health care entities, and may hinder entry by potential PHR providers. In this manner, these laws can lead to higher prices and reduced consumer choice.

Although consent and breach notification requirements appear likely to retard HIT adoption, the benefits they provide appear primarily to be non–tangible; both types of requirements allow consumers to exercise some dominion over their health information by providing them a veto over who sees it in the ordinary course of business and notifying them when unauthorized access occurs. That suggests that policy makers need to develop a clearer understanding of consumers' underlying preferences for privacy and how these preferences vary throughout the population—and perhaps across treatment contexts—before undertaking costly regulations that appear to provide very modest tangible benefits.[317] Further, theoretical commitments about the foundations of privacy rights, or the nature of privacy interests, cross–cut questions about the ideal scope of privacy protections, the resources that ought to be devoted to privacy protections, or how best to tailor privacy protections to minimize harm to other important interests. Autonomy–based privacy rights principles may suggest a property rights regime under which medical information belongs to patients, with providers enjoined from sharing PHI with third parties without consent, but we should be wary of conclusory suggestions that the precise metes and bounds of such rights would be obvious. We suggest that until there is better information on the distribution of privacy preferences, policy makers should exercise special caution when considering new or extant consent and breach notification requirements.

In light of the current state of knowledge of patients' privacy preferences, we offer regulatory reform proposals for consent, breach notification, and data security requirements. We make these suggestions mindful that the federal government is not the only player in this policy

. . . [as they are] for white deaths." Miller, *supra* note 21, at 233. It was predicted that eMR adoption, in that context, would cost roughly $450,000 per infant life saved. *Id.* at 234.

316. *See supra* notes 57–61 and accompanying text.

317. *See* Koetting, *supra* note 295, at 707 ("[W]e appear on the verge of incurring large expenses from limited health care funds and/or inhibiting appropriate access to medical information for solutions that have a low likelihood of solving the problems that are at the heart of people's concerns.").

space. Indeed, the variation in state privacy regulations gives rise to the result that overly–stringent or inconsistent privacy laws can impede HIT adoption. Thus any approach inevitably has to grapple with the issue of federalism, which we leave for Part VI.

One possible path forward for consent requirements would be to retain the Privacy Rule's carveout for treatment purposes, but also allow patients to opt out of HIT systems on a provider–by–provider basis. After a provider has joined an interoperable HIT network, it would give its patients the option to have their records sequestered from the shared system (both retroactively and prospectively). This approach to consent has at least three advantages. First, the Privacy Rule's treatment exception appears to be a good candidate for a majoritarian rule because it is unlikely that many consumers would object to providers sharing their medical information to enable treatment.[318] Survey evidence suggests that most patients are comfortable with the current treatment of medical records by their health care providers,[319] and although they have concerns about the privacy implications of HIT, they believe that the benefits from HIT outweigh the privacy risks.[320] More generally, since the early 1990s, a majority of consumers have described themselves as either "privacy unconcerned" or "privacy pragmatists," who are willing to permit the use of their personal information in return for a benefit and sufficient safeguards.[321] Only around a quarter of the population can be described as "privacy fundamentalist," who feel that their privacy rights are not being handled correctly, desire only an opt–in rule, and are unwilling to trade

318. *See* Terry & Francis, *supra* note 11, at 703 (arguing that consentless information flows be limited to providers within a patient's "circle of care," which includes "practitioners that are immediately and directly involved in the care of the patient—and on an as-needed basis with another member of a patient's medical team"); Sunstein, *supra* note 200, at 712 (arguing that the presumption in favor of patient control over private information should be rebutted when disclosure is to other doctors on a patient's "medical team" because "if this is necessary for good treatment, the patient has no reasonable basis for complaint").

319. *See Harris Poll*, *supra* note 195 (showing 70% of patients surveyed agree that they are satisfied with the way that doctors and hospitals treat their personal health information, and 63% agree that the increased use of computers to record and share patient medical records can be accomplished without jeopardizing proper patient privacy rights).

320. *See* Beckey Bright, *Benefits of Electronic Health Records Seen as Outweighing Privacy Risks*, WALL ST. J., Nov. 29, 2007, *available at* http://online.wsj.com/article/SB119565244262500549.html (reporting results from a Wall Street Journal Online/Harris poll that finds although 51% (down from 61% in 2006) of those surveyed believe that the use of electronic medical records makes it more difficult to ensure patient privacy, 60% (and 72% of those that currently use electronic medical records) agree that the benefits of electronic medical records outweigh the privacy risks).

321. *See* Beales & Muris, *supra* note 16, at 118 (noting that the majority of consumers are privacy pragmatists who are "willing to provide information in exchange for benefits"); Westin, *Opinion Surveys*, *supra* note 208 (noting that since the early 1990s consumers have split into three groups: Privacy Fundamentalists (25%); Privacy Pragmatists (63%), and Privacy Unconcerned (12%)).

privacy protections for benefits.[322] These data suggest that most patients are satisfied with the status quo and are willing to allow providers to share their health information in return for benefits.

Second, maintenance of the Privacy Rule would allow high and low–demanders for privacy to self–select into different regulatory regimes rather than force patients to pool into a regime that provides either inefficiently high or low levels of privacy. Because those who opt out would internalize the costs of their decisions, in terms of lost HIT benefits, they would do so only if they value their privacy more highly than those benefits.[323] The remainder of the population, who are willing to accept the Privacy Rule's requirements, will also enjoy the full benefits of HIT, whatever they prove to be.[324] Although the choice of default position is irrelevant in a world without transaction costs,[325] in the real world an opt–in default is likely to be more efficient than an opt–out default. As noted above, it is likely that the majority of patients would choose to participate in HIT networks under the status quo. An opt–in default would economize on aggregate transaction costs by requiring fewer people to make a decision. Further, it may be costly to make an opt-in/opt-out decision and the opt–in default is likely to cause less harm.[326]

Third, by eliminating consent for individual information requests for treatment purposes, this approach would not affect the marginal cost of the flow of information.[327] It is important to note, however, that this result is only obtained if opt–out occurs at the provider level. If the general regime were to allow privacy–sensitive patients to require their providers to obtain and document consent for each discrete instance of information

322. *See id.*; *Harris Poll*, *supra* note 195, at 1 ("[A]bout 25 percent of the public consistently feels that their legitimate privacy rights are not being handled properly by business, employer, or government organizations.").

323. Indeed, the opt-out choice would not necessarily be so stark, as it would provide high-demanders for privacy two sorts of choices: they could opt out of HIT systems generally, internalizing the costs implicit in opt-out decisions, but they could also choose ad hoc use of HIT systems in particular contexts in which private assurances or protections more closely matched their preferences (for example, in a particular practice setting, or with a utility, where special protections substantially exceeded those given publicly).

324. For example, these opt-out patients would not enjoy monetary and non-monetary benefits from enhanced communication among health care providers to coordinate care. *See* Terry & Francis, *supra* note 11, at 701–02. They would, of course, enjoy some, as public health or various benefits accruing to the public fisc would be at least partly available to the larger population, although we should acknowledge that, at the margin, these may be diminished according to the number of opt-outs.

325. R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 15 (1960).

326. *See* Beales & Muris, *supra* note 16, at 114–18 (discussing how, in the context of consumer financial information, the informational costs of exercising choice regarding whether to opt-in to or opt-out of an information-sharing regime can swamp expected benefits, such that the default position often becomes the status quo).

327. *See* Terry & Francis, *supra* note 11, at 703.

sharing (even for legitimate treatment or reimbursement purposes) or to demand other *ad hoc* mandates—say, to select certain records or parts of records from providers to be excluded from the HIT network—that would foist costs on those remaining in the system by suppressing network externalities, and thus HIT adoption rates.[328] Further, it would reduce providers' willingness to rely on electronic records for treatment decisions to the extent that they have concerns about accuracy, which would also raise costs and reduce HIT adoption rates.[329] Finally, allowing patients to opt–out of the system on a record–by–record (or information within a record) basis would impose additional recordkeeping costs on providers, which likely could not be charged only to those who request the segregation of their information but, instead, would be built into everyone's charges.

With respect to breach notification, triggers based on the relative risk of harm to consumers, rather than on mere incidence of access also appear to strike a desirable balance. For example, the FTC's proposed breach notification rule for PHRs moves in this direction by requiring notification only when the breach involves *unencrypted* data and allowing PHR vendors to rebut the presumption that breached data has been acquired.[330] This proposal, for example, would relieve a PHR vendor from the burden of notification when a staff member inadvertently accesses a database.

Substitution away from consent and breach notification requirements into data security requirements may be more efficient. Because the former species of regulation implicate marginal costs of data transmission, they risk deterring beneficial sharing of health information. On the other hand, data security requirements implicate primarily (if not exclusively) fixed costs. Thus, these requirements may be more efficient than other forms of regulation to assure patient privacy from an error-costs perspective.

Finally, although the preceding discussion has focused entirely on optimal types of regulation, it is worth exploring the extent to which government intervention is needed at all. The Constitution clearly protects citizens from unwarranted government collection and government-mandated disclosures of private information,[331] and is likely to prohibit the state from setting a ceiling on the privacy protections that

328. *See id.* at 702–03.

329. This is a concern that has been raised about some approaches to PHRs, or PHR/eHR interfaces. *See* Dimitropoulos and Rizk, *supra* note 14, at 430; Koppel, *supra* note 56.

330. Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,915–16 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).

331. *See* Whalen v. Roe, 429 U.S. 589, 599 (1977); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 570 (3rd Cir. 1980).

private parties may provide, for example, by mandating disclosures without consent.[332] There is, however, no Constitutional mandate for the government to set a privacy floor for private entities.[333] Private entities face competition in the marketplace. To the extent that health care providers and HIT vendors compete over privacy protections, the need for regulation may be diminished. In other areas of the economy, there is evidence that firms are aware that consumers value privacy and that firms compete on this dimension.[334] If evidence of direct competition on this dimension of services is slight in the health care arena, it is nonetheless important to note that, for example, private PHR providers have expended resources on better understanding consumer knowledge and preferences. Microsoft, Google, Kaiser, and others prominently display their privacy policies on their PHR web sites.[335] The primary online PHRs are free and consequently generate revenue by attracting traffic for advertisers. In such double–sided markets, when something (*e.g.*, over–the–air television, information or entertainment on a Web site) is given away to consumers, competition necessarily occurs in non–price dimensions to attract "eyes" or views. These corporate displays are one example.

In many instances, regulation or liability is premised on informational asymmetries. It may be reasonable to assume that consumers are poorly positioned to appreciate all the risks associated with certain products, such that the market alone may fail to produce efficient precautions or levels of safety.[336] By contrast, in the face of information problems that cause them to overestimate their risks, consumers may demand "too much" privacy. For example, a large percentage of consumers say that

332. *See* Citizens for Health v. Leavitt, 428 F.3d 167, 180 (3rd Cir. 2005).

333. *Id.*

334. *See*, *e.g.*, Peter Swire, Antitrust, Privacy, and Other Non-Price Competition, ICOMP Conference on Privacy Competition in the Online Market Place (Apr. 27, 2009), http://www.i-comp.org/calendar/downloadFile/97 (describing how Google, Yahoo, Microsoft, and Ask compete over privacy features for search engines and how Facebook and MySpace compete over privacy for social networks); PAUL H. RUBIN & THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION 40–42 (2002) (cataloging examples of the market disciplining firms for violating consumers' preferences for privacy).

335. In addition to a link to its "full Privacy Statement," prominently displayed on the opening page of Microsoft Health Vault's site for personal use, is the following: "Our HealthVault Privacy Principles: • You control the Microsoft HealthVault record you create. • You decide what goes into your HealthVault record. • You decide who can see, use and share your information. • Microsoft won't use your information in HealthVault to personalize ads or services without explicit permission." Microsoft HealthVault, http://www.healthvault.com/Personal/index.html (last visited Mar. 26, 2010); Google Health, Take Charge of Your Health Information, https://health.google.com (last visited Mar. 26, 2010); Kaiser Permanente, Privacy Practices for Our Web Site, https://members.kaiserpermanente.org/kpweb/entryPage.do?cfe=072 (last visited Mar. 26, 2010).

336. *See* SHAVELL, *supra* note 287, at 214–15.

they mistrust HIT, but an even larger percentage reports that they are relatively ignorant about HIT.[337] Similarly there appears to be a mismatch between consumer fears of loss from identity fraud after a breach and actual levels of harm.[338] These data indicate that consumers probably overestimate actual risk of harm associated with HIT and are unaware that HIT may tend to make records safer rather than more vulnerable. Further, it is dubious that patients are generally aware that stringent consent and breach notification requirements are likely to have a negative impact on HIT adoption and use. Thus, there are good reasons to be concerned that the market may produce "too much" privacy, and that the current level of demand for regulation to protect the privacy of electronic health information is greater than it would be in a world of perfect information. Politicians—who may be susceptible to some of the same information costs—may thus be biased toward over–regulation; some more knowingly may be tempted to take advantage of consumers' (and voters) relative lack of knowledge to push through self–aggrandizing, but harmful privacy regulations. As Professor Sunstein notes, in the face of "isolated but highly publicized cases, . . . [p]olicy entrepreneurs, including candidates interested in reelection and good publicity, might well seek increasingly severe controls."[339] These informational issues again admonish policy makers to be cautious when developing privacy regimes to govern HIT. At the very least, policy defaults ought to be set to favor clarity over opacity, and to avoid disutility based on needless cues to information problems or counter–productive decision making biases.[340]

IV. PREEMPTION VERSUS FEDERALISM IN PRIVACY REGIMES

Leaving aside the stringency of any particular state regulatory regime, there are also costs associated with the patchwork of regimes. Although allowing states to experiment with different approaches to privacy is likely to have benefits, it also comes at a cost. Inconsistent state

337. *See* NATIONWIDE SUMM., *supra* note 13, at 6-39 (showing that although nearly half of consumers surveyed were apprehensive about using electronic health records, 57% reported not having "read, seen, or heard" anything about electronic health records prior to the survey, which suggests "a fundamental information gap about electronic health information exchange within the general consumer population").

338. *See* PONEMAN INST., CONSUMERS' REPORT CARD ON DATA BREACH NOTIFICATION 5 (2008) (reporting that while 32% of those surveyed believed that following a data breach their likelihood of becoming an identity fraud victim was greater than 40%, the actual incidence of fraud was 2%, which suggests "consumers' fears about the possibility of becoming an identity theft victim do not reflect the actual rate of experience").

339. Sunstein, *supra* note 200, at 713.

340. *See generally*, RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (Yale Univ. Press 2008).

privacy laws can impede cross–border communication of health information and can increase the cost of designing and implementing HIT systems.

There appears to be broad recognition—even in the states themselves—that much is at stake in furthering interoperable HIT and that the current mix of state laws may be a serious barrier to doing so. For example, 42 states are now working in various consortia—under the auspices of the Health Information Security and Privacy Collaboration (HISPC)[341]—at diverse tasks aimed at furthering the flow of electronic health information, including efforts at harmonizing state health privacy and data security law.[342] Participants in these efforts have observed not only that "[m]any states have a series of antiquated, fragmented, and non–standardized laws that may unintentionally create a barrier to the appropriate exchange of electronic health information," but that "comprehensive reform would be a resource-intensive task in most states."[343]

A national study prepared for HHS observes that,

> Relevant laws and regulations developed and evolved largely in response to the paper–based health information exchange. Legal restrictions addressing health information exchange were often dispersed across many different statutes and regulations and are sometimes inconsistent with one another. Several states reported that antiquated laws written for paper–only environments created significant barriers to electronic health information exchange. Other states noted that laws were silent with respect to certain aspects of health information exchange, leading to varied business practices and customs.[344]

341. HISPC was established through a contract with HHS to address the privacy and security challenges presented by electronic health information exchange through multistate collaboration . . . Each HISPC participant had the support of its state or territorial governor and maintained a steering committee and contact with a range of local stakeholders to ensure that developed solutions accurately reflect local preferences. RTI INT'L HEALTH INFO. SECURITY & PRIVACY COLLABORATION (HISPC), http://www.rti.org/brochures/Health_Info_Security.pdf (last visited Mar. 26, 2010).

342. *See generally* Health Info. Security & Privacy Collaboration (HISPC) Nat'l Conference, Bethesda, MD (Mar. 4–6, 2009) (conference agenda and other materials are available at http://www.rti.org/events.cfm?bgnyear=2009 (follow the "Health Information Security and Privacy Collaboration (HISPC) National Conference" hyperlink)). It should be noted that such consortia organized under HISPC tend to be smaller than national in scope. For example, at the March 2009 conference there was a report on harmonization efforts undertaken by an 11-state consortium chaired by Indiana. *Id.*

343. Julie Roth, Christina Stephan & Patricia Gray, Harmonizing State Privacy Laws for HIE, Health Info. Security & Privacy Collaboration (HISPC) Nat'l Conference (Mar. 5, 2009), http://www.rti.org/files/hispc/Harmonizing_State_Privacy_Law.pdf. *See supra* note 342.

344. NATIONWIDE SUMM., *supra* note 13, at 6-3.

For all of that, relatively little attention has been paid to the possibility of preempting state law requirements in this area. To be sure, a few commentators have recommended the express preemption of state health information privacy laws, generally because they see the requirements—and the task of compliance with them—as exceedingly complex or otherwise burdensome for health care providers or other business entities.[345] But more general considerations of the costs imposed within and across bodies of state law have been few, and many broad-ranging HIT policy discussions are silent regarding the possibility of preemption. For example, the HHS report mentioned in the preceding paragraph considers various state law issues and means of addressing them, and does not mention the possibility of broader preemption of state law.[346] At the 2008 FTC Workshop, three panels of participants addressed HIT–related issues, each incorporating privacy issues into its discussion, but no participants discussed the policy option of preemption, not even for the purpose of rejecting it.[347] The Recovery Act generally retains the very limited sort of preemption contemplated under HIPAA,[348] under which the states may not waive the minimum requirements of HIPAA and the federal Privacy Rule, even as they are free to regulate unchecked "above" those minimum requirements.

There may, of course, be reasons to advocate for state health privacy regulation, whether favoring particular requirements or the maintenance of state prerogatives. First, as consumers may be harmed by violations of their health information privacy, and as they may be poorly situated to

345. That is not to suggest that it has never been mentioned. *See Testimony on the Proposed Rule on Confidentiality of Patient Records: Hearing on Health Insurance Portability and Accountability Act Before the S. Comm. on Health, Education, Labor and Pensions* 106th Cong. (2000) (testimony of Joanna C. Horobin, Executive Vice President For Commercial Development, EntreMed Inc.) (suggesting the patchwork of state regulations is unworkable, and calling for new federal legislation that generally preempts state medical privacy law); Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 105–06 (2007) (advocating new federal law that "must contain an express preemption clause stating that the legislation is intended to serve as a ceiling as well as a floor"); *cf.* Nicolas P. Terry, *An eHealth Diptych: The Impact of Privacy Regulation on Medical Error and Malpractice Litigation*, 27 AM. J.L. & MED. 361, 368 (2001) ("[T]he unsatisfactory 'more stringent' partial preemption provision [in current force] is likely to befuddle and annoy healthcare institutions with interstate businesses for years into the future. There may be even worse to come as state legislators are prodded by dissatisfied privacy advocates to pass statutes that fill perceived gaps in the PIHI regulations, thereby increasing the number of non-preempted protections.").

346. *See* NATIONWIDE SUMM., *supra* note 13. The term "preemption" does appear in the report, albeit in a different context.

347. *See* Address at FTC Workshop on Innovations in Health Care Delivery (Apr. 24, 2008) (transcript available at http://www.ftc.gov/bc/healthcare/hcd/docs/hcdwksptranscript.pdf).

348. American Recovery and Reinvestment Act of 2009 (Recovery Act), § 13421(a), 123 Stat. 115, 229 (2009).

provide (or contract) for protection against such harms, one may be concerned about the general question of the adequacy of the larger set of federal and state privacy regulations. At the FTC Workshop, panelists were generally in agreement that privacy concerns were important to HIT policy, and although some panelists were especially concerned about the costs of excessive regulation, others described the then–current mix of federal and state regulation as insufficiently protective of consumers' interests.[349]

It also could be argued that the states may offer an important "laboratory" for testing various regulatory responses to the problems presented by emerging or rapidly changing technologies. For example, Bruce Kobayashi and Larry E. Ribstein have argued that state consumer privacy law is generally superior to federal law in the realm of digital information precisely because of the dynamic nature of the underlying technologies and consumers' interaction with them.[350] Where consumers' expectations of privacy remain unclear, there may not be a set of common, baseline costs and benefits associated with certain industry practices that is adequate to justify uniform federal law. State law, on the other hand, "emerges from 51 laboratories and therefore presents a more decentralized model that fits the evolving nature of the Internet . . . . [and] competition among state laws can mute the inefficient tendencies of interest group legislation."[351] In addition, "[t]he U.S. government's regulation of privacy rights could determine important aspects of the Internet's structure and reduce the flexibility and openness that has made the Internet a major economic force."[352]

The argument is far from decisive in the present case. First, we should note that Kobayashi and Ribstein expressly decline to extend their argument about the potential superiority of state law to the area of medical privacy. They distinguish "information that consumers clearly

349. *Compare* Pritts, *supra* note 86, at 287 ("People] will not adopt it [HIT] if there is not adequate trust that their information will be kept confidential."), *with* Miller, *supra* note 21, at 231, 233 (regarding costs of state law privacy protections—impact on HIT adoption and relationship between HIT adoption and neonatal mortality, respectively); Dente, *supra* note 50, at 274 (discussing the need to think about health needs and the importance of information "when we balance the need for connectivity, interoperability, information, with the rights of all of us to have . . . patient privacy"). *Cf.* Trenkle, *supra* note 177, at 281 ("[A] lot of things need to be balanced against privacy and security needs . . . . [But] it is not an either/or, it is something that needs to be worked together.").

350. *Cf.* Bruce H. Kobayashi & Larry E. Ribstein, *A Recipe for Cookies: State Regulation of Consumer Marketing Information*, GEO. MASON L. & ECON. RES. PAPER NO. 01-04, Feb. 2001, at 5–6 (arguing, on these grounds, that state consumer privacy law is generally superior to federal law, although expressly declining to extend the argument to medical privacy).

351. *Id.* at 5.

352. *Id.* at 4.

expect to be kept private, such as medical records . . . [from information] where such expectations are much less clear."[353] Presumably, if—ranging across the states—there are strong, background expectations of privacy regarding personal information in consumer medical records, the interest in having varied experimental responses to situations where such expectations are denied is considerably diminished.[354]

Second, where Kobayashi and Ribstein would apply their argument, it depends on the notion that "competition among state laws can mute the inefficient tendencies of interest group legislation."[355] Perhaps this is true, but that also depends on the extent to which there can be such competition among state laws. With Internet privacy, crucial competitive mechanisms seem to be (a) enforcement, by the courts, of choice of law and choice of forum clauses and (b) the ability of web operators to "block transmission to states that do not enforce contractual choice."[356] Even in the more general realm of Internet privacy, "a" may be an unlikely counterfactual and "b" seems at least costly and very likely intractable. To the extent that the flow of information is not readily cabined, and where choice of law may be at issue, there may be reasons to wonder whether regulatory reach will be at least as powerful as regulatory competition. In this regard the U.S./E.U. experiences with data privacy law generally may be instructive, and at least one commentator has argued that there are conditions under which the regulatory interests of small states can prompt larger ones to "ratchet up" their regulatory requirements, even to some extent past their own perceived interests (and independent of the question whether one or another state had stumbled upon more efficient requirements).[357] Rejecting the notion that global IT competition prompts a regulatory race to the bottom, Professor Shaffer suggests that, although "it is not a race to anywhere in particular, it can (more likely than not) give rise to a ratcheting up of national standards. This is particularly the case where foreign regulation has externalities, as is the case with data privacy protection."[358]

Further, public choice problems may sometimes be exacerbated—not ameliorated—at the state level. For example, for many issues,

353. *Id.* at 5.

354. Of course the extent to which they are diminished may vary. Certainly, there may be significant heterogeneity in consumer preferences, interests, or expectations above some shared baseline, and the extent to which any particular regulatory regime satisfies either baseline needs or varied ones may be in question.

355. Kobayashi & Ribstein, *supra* note 350, at 5.

356. *Id.* at 5–6.

357. Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 5–8 (2000).

358. *Id.* at 7.

national stakeholders may be able to identify seed states in which lobbying costs are relatively low, countervailing business interests are relatively diminished, and—as is often the case—consumer interests are diffuse and costly to organize. Success therein achieved may be more than local: it may tend to lower the costs of lobbying in other states, producing, in efficient fashion (for the lobbying stakeholder), a sort of legislative cascade.[359]

Finally, the notion of vigorous competition aided by the threat of virtual exit seems an especially poor fit in many health care contexts. Informed and well–counseled corporate parties may, for example, engage in arms–length negotiation over choice-of-law clauses on the basis of good and tolerably symmetric information about their own interests and the relevant choices of law.[360] One may be less optimistic about such negotiations between large national payers, mid–sized regional or local providers, and individual patients, given an industry with notoriously poor price and quality information transparency,[361] where both provider practices and consumer expectations about such practices may be highly variable, and when individual patients may require real-time trauma treatment from a hospital with no local competition.

Of course, even to the extent that a poor fit between certain bodies of state law may be costly, there are other possible policy responses besides expanding the preemptive reach of HIPAA. Harmonization efforts are, as

359. Without analyzing the factors behind any particular legislative cascade, we may observe, nonetheless, that it is not uncommon for similar legislation to be adopted across many states following a legislative success in one particular state. For example, California was the first to enact a data breach notification law, requiring companies to notify California residents whose unencrypted personal information was acquired by an unauthorized person. *Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Sci. and Transp. on Data Breaches and Identity Theft*, 109th Cong. 11–12 (2005) (Congressional testimony by FTC Chairman Deborah Majoras on data breaches and identity theft, discussing the California breach notification law, CAL. CIV. CODE § 1798.82), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf. Many states followed California's lead, and to date, 32 states have some form of data breach notification. We do not suggest that the states had no reason to be concerned about breach notification issues. We suggest, simply, that the progress of follow-on legislation across the states often proceeds at a pace that suggests something other than the application of policy experiments observed in different jurisdictions, not least because the pace of adoption makes it implausible that the costs and benefits of legislation, and its implementation, by early adopters has been analyzed by subsequent ones.

360. It may be, as well, that where market transactions commonly involve parties thusly situated, there is competitive pressure in favor of the convergence of state law regimes on a relatively efficient model, perhaps as we have seen with the dominance of Delaware corporate law.

361. *See, e.g.*, Robert Wood Johnson Found., *Choosing a Health Care Provider: The Role of Quality Information*, Policy Brief No. 14 (May 2008), *available at* http://www.rwjf.org/files/research/051508.policysynthesis.qualityinfo.brief.pdf; A DOSE OF COMPETITION, *supra* note 69.

noted, underway within consortia of states, as well as other possible state law reforms. But harmonization is a costly process in itself,[362] and the results of considerable efforts under the auspices of HISPC over the past several years—although in many regards interesting—seem partial and limited.

Wyeth v. Levine[363]—addressing very different health care policy and legal issues—may provide an interesting contrast with present preemption considerations. In that case, petitioner argued that state law claims, sounding in tort, that alleged a failure to adequately warn of the risks attending use of a drug product (administered in a particular way), were preempted by the regulatory oversight of the federal Food and Drug Administration (FDA)—in particular, by the approval of the marketing of the drug product, as safe and effective, under particular labeling, under the federal Food, Drug, and Cosmetic Act (FDCA).[364] The Court held that they were not.[365]

Analogous implied preemption arguments are not available under HIPAA, the federal Privacy Rule, or the Recovery Act, because the question whether HIPAA may impliedly preempt more stringent state law requirements is rejected, expressly, by HIPAA itself. Regulations promulgated under HIPAA with regard to "the privacy of individually identifiable health information . . . shall not supercede 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."[366] The interesting policy question, rather, comes in two parts. First, if the preemption/non–preemption provision did not exist, would colorable—or perhaps persuasive—implied preemption arguments be available to stakeholders burdened by state health privacy laws? Second, if so, to what extent might such arguments work as policy grounds for the express preemption of such state laws?

The Court's contentious decision in *Wyeth*[367] rests on the rejection of two separate implied preemption arguments.[368] First, the Court rejected the

362. *Cf.* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1319–20 (2000) (regarding difficulties and harms of harmonizing privacy rules across national borders).

363. 129 S. Ct. 1187 (2009).

364. *Id.* at 1193–94.

365. *Id.* at 1190.

366. Health Insurance Portability and Accountability Act of 1996 (HIPAA) § 264(c)(2), 110 Stat. 2033–34, 42 U.S.C. § 1320d-2 (2009).

367. Writing for the minority, Justice Alito wrote, "[t]his case illustrates that tragic facts make bad law," and argued that, "[i]n its attempt to evade *Geier*'s applicability to this case, the Court commits both factual and legal errors." 129 S. Ct. at 1222 (Alito, J., dissenting) (citing Geier v. Am. Honda Motor Co., 529 U.S. 861 (2000)).

368. *Id.* at 1193.

conflict preemption argument that, "it would have been impossible for [Wyeth] to comply with the state law duty . . . without violating federal law."[369] Although the FDA has the power to approve (or reject) proposed or extant labeling for a prescription drug product, FDA regulations do permit certain provisional changes to reflect "newly acquired information" upon the manufacturer's filing a supplemental application with the FDA (but prior to approval of that supplemental application).[370] More generally, the Court identified what it saw as "a central premise of federal drug regulation that the manufacturer bears responsibility for the content of its label at all times."[371] Hence, federal regulations—and in the *Wyeth* case, administrative decisions reached under those regulations—do not determine the appropriate level of warning. The appropriate level of warning is to be determined by the manufacturer, subject to FDA review.

Absent HIPAA section 264, a different argument might be made about health information privacy. On the one hand, health care providers and other covered entities are free in various ways to implement their own privacy policies. On the other hand, no such entity can make unilateral changes—pending HHS approval or otherwise—to the basic requirements of HIPAA and the Privacy Rule; neither can it modify the rights HIPAA grants to patients and their representatives. There is, therefore, specific content to the requirements of federal law in the privacy case, and private parties may comply or fail to comply with those requirements, but they may not change them.[372] In brief, whereas drug manufacturers—at least arguably—may disclose certain new risk information prior to administrative approval, health care providers may not disclose protected PHI, as proscribed under HIPAA and the Privacy Rule, without authorization.

Second, the Court rejected Wyeth's argument that state law decisions regarding the adequacy of the labeling in question "would obstruct the purposes and objectives of federal . . . regulations."[373] Against that possibility, the Court noted the absence of an express preemption provision in the FDCA. The Court also rejected the FDA's own view that the FDCA establishes "both a 'floor' and a 'ceiling' so that FDA approval of labeling . . . preempts conflicting or contrary State law."[374] Rather, the Court

369. *Id.* (holding otherwise at 1199).

370. *Id.* at 1196.

371. *Id.* at 1197–98.

372. As noted above, pertinent federal law includes not just HIPAA and the federal Privacy Rule but also the FTC Act and the Recovery Act.

373. *Wyeth*, 129 S. Ct. at 1193 (holding otherwise at 1204).

374. *Id.* at 1200 (internal quotations omitted) (citing 71 Fed. Reg. 3922, 3934–35 (2006)).

preferred the FDA's older (and contrary) view that federal standards are "a floor upon which States could build."[375]

Plainly, Congress now intends that HIPAA function as a floor, but not a ceiling, for health information privacy protection. But Congress also intends that, in general, the Office of the National Coordinator for Health Information Technology (ONC) carry out its duties "in a manner consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information."[376] In particular Congress has declared that ONC activities will be directed toward "the utilization of an electronic health record for each person in the United Sates by 2014."[377] Considerable appropriations have been devoted to those HIT policy goals. To the extent that there is, as we have discussed, some tradeoff between state law protection of health information privacy and the rate of HIT adoption, the following question presents itself: If the costs of additional state law protections for health information privacy are substantial and "[m]any states have a series of antiquated, fragmented, and non–standardized laws that may unintentionally create a barrier to the appropriate exchange of electronic health information," while "comprehensive reform would be a resource intensive task in most states,"[378] what is the point at which state law regulation of health information privacy may frustrate the larger purpose of the Recovery Act's HIT provisions?[379]

Field preemption, another type of implied preemption, may also be an interesting issue for policy purposes. Congressional intent to preempt state law may be inferred "where the scheme of federal regulation is sufficiently comprehensive to make reasonable the inference that Congress 'left no room' for supplementary state regulation."[380] Such cases are not unrelated to preemption arguments resting on the purposes and objectives of federal law, in that the Court has held that Congressional intent to preempt state law may be inferred where "the federal interest is so dominant that the federal system will be assumed to preclude enforcement of state laws on the same subject."[381] Even though HIPAA was not intended, as drafted, to establish comprehensive health information privacy protection,

375. *Id.* at 1202.

376. American Recovery and Reinvestment Act of 2009 (Recovery Act), § 3001(b), 123 Stat. 115, 229 (2009).

377. *Id.* at § 3001(a)(3)(A)(ii).

378. Roth et al., *supra* note 343. *See supra* note 342.

379. The Recovery Act provides that its two central HIT titles—tit. XIII of div. A and tit. IV of div. B—be referred to as the "Health Information Technology for Economic and Clinical Health Act" or the "HITECH Act." Recovery Act § 13001.

380. Hillsborough County v. Automated Med. Labs., Inc., 471 U.S. 707, 713 (1985) (quoting *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947)).

381. *Rice*, 331 U.S. at 230.

between the adoption of HIPAA and the adoption of the Recovery Act, many nonetheless would have viewed field preemption arguments as problematic in this context. For example, participants in the FTC Workshop and other commentators had expressed concerns about possible gaps in HIPAA,[382] especially with regard to the treatment of business associates[383] and, more recently, in the emerging area of PHRs.[384] As we have noted, however, the Recovery Act comprises provisions that address these substantial gaps with requirements (and possible penalties) pertaining to business associates,[385] new requirements pertaining to PHR vendors and related entities,[386] and provisions for new rule making in these areas by HHS and the FTC.[387] The Recovery Act also calls for further study, directly by federal agencies and otherwise under federal aegis, with additional recommendations to Congress presumed to be forthcoming. If federal regulation does not (or will not soon) occupy the field, at what point might it?

There is no sure answer to the question whether the elimination of HIPAA's Section 264 would establish the likely success of implied preemption arguments in the area of health information privacy. It may be that *Wyeth* has raised the bar for such arguments generally, but the extent to which the Court will read its holding to cabin more than the reach of the FDCA with regard to state law claims about drug labeling remains to be seen. Such implied preemption arguments would be difficult in any case, especially to the extent that the Court found applicable, and persuasive, the general notion that "the historic police powers of the States [are] not to be superseded by . . . Federal Act unless that was the clear and manifest purpose of Congress."[388] One might also suggest that the substantial structural complexity of the Court's implied preemption doctrine is exceeded greatly by the complexity of the doctrine's semantics—how it might be applied to novel circumstances is less clear than it could be. Possible implied preemption arguments do, however, point to policy grounds to consider express preemption. In brief, it is not clear that the

382. *See, e.g.*, McAndrew, *supra* note 118, at 211 (regarding "certain gaps in the current HIPAA coverage"); McGraw, *supra* note 31, at 146–47 ("gap" in HIPAA coverage); Pritts, *supra* note 86, at 289 ("gaps" in federal and state privacy protections).

383. McGraw, *supra* note 31, at 146 (identifying this as a "gap" in HIPAA); *cf.* McAndrew, *supra* note 118, at 211–12 (noting many concerns about the lack of "level playing field" with business associates and how business associates handle PHI).

384. McGraw, *supra* note 31, at 146–47 (regarding "gaps" in HIPAA coverage, especially with regard to personal health records).

385. *See* American Recovery and Reinvestment Act of 2009 (Recovery Act), §§ 13401, 13404, 123 Stat. 115, 229 (2009) (regarding the application of security provisions and penalties and the application of privacy provisions and penalties, respectively).

386. *Id.*§ 13407.

387. *See supra* note 104 and accompanying text.

388. *Wyeth v. Levine*, 129 S. Ct. 1187, 1194–95 (2009) (internal citations omitted).

web of state privacy and data security protections can be read consistently with federal privacy, data security, and HIT law, not least because it cannot be read consistently on its own—often, it seems, even the prospects of intrastate harmonization may be unclear. Moreover, it may be that the larger body of state law is at odds with the balancing of policy goals sought in federal HIT law. In particular, the Recovery Act's HIT provisions appear to balance substantial interests in health privacy against substantial interests in the development and adoption of interoperable HIT and, more than that, the actual flow of health information on a national basis. State law provisions do not appear to strike a similar balance, and it is not clear that they could. That is not simply a matter of adding or subtracting cost to the acquisition of HIT hardware and software or moving a metaphorical floor or ceiling up or down, but about optimizing a complex set of considerations about health care practice, health care funding, standard setting and certification, and more. The interplay between the HIT policy and standards advisory committees noted above should be instructive in this regard. Indeed, this Article more generally illustrates the complexity of benefits and barriers that may be associated with HIT, and the interrelationships between them. Interleaving extant—and changeable—state regulatory schemes into this developing matrix is likely a herculean task, supposing it is tractable at all.

CONCLUSION

Health information technology shows great promise, but it will be costly to implement on a national scale. By providing significant financial incentives, the recently enacted Recovery Act will further HIT adoption greatly, but significant non–financial barriers remain. Perhaps the paramount regulatory barriers are those designed to protect privacy. Consumers clearly value health information privacy—both for the sake of maintaining autonomy over intimate details of their lives and because they worry about financial and physical harms that can come from data breach. The extant mix of federal and state regulations—chiefly consent requirements and, to a lesser extent, breach notification requirements—also impede HIT adoption by making it more costly to share health information via interoperable systems. At the same time, many privacy regulations do not appear to provide net benefits, at least in terms of the tangible harms they seek to suppress. Because most benefits are likely to be intangible, a regulatory regime that strikes the correct balance between privacy and HIT adoption can only follow a richer understanding of patients' intrinsic valuations of privacy, which are likely to vary across

the population and contexts of care. Further, given that consumers clearly are concerned about their medical privacy—perhaps overly so—the market should not be discarded as a source of privacy protection.

Calibrating the correct mix of state and federal health privacy regulation also requires balance. Allowing health privacy regimes to vary across states permits experimentation and regulations that more closely match local privacy preferences, to the extent that preferences vary on a state level. These benefits, however, increase the cost of developing and implementing interoperable HIT on a national scale, as well as the cost of the flow of health information over channels already established. Although HIPAA expressly sets only a federal floor of privacy protection, the recent federal push behind HIT adoption on a national scale, combined with HIPAA and Recovery Act privacy provisions, suggest at least a policy rationale for reconsidering the federal preemption of state health privacy laws.