2002

Medical Records and HIPAA: Is It Too Late to Protect Privacy

Peter D. Jacobson

Medical Records and HIPAA: Is It Too Late to Protect Privacy?

Peter D. Jacobson†

In 1999, Sun Microsystems CEO Scott McNealy stated that consumer privacy issues are a "'red herring.'"[1] When asked about privacy, he said, "'You have zero privacy anyway. Get over it.'"[2] Even if McNealy overstates the end of privacy, there seems little doubt that it is increasingly difficult to maintain control over one's personal data. By combining publicly available data from various sources, resourceful sleuths can easily develop a personal profile of most citizens that many of us would prefer not to make available to our neighbors. Litigation consultants, for example, compile profiles of potential jurors based on publicly available data. The same technology that allows this Article to be submitted via the internet allows others to track my internet browsing preferences. Even the judiciary, usually regarded as a bulwark against the invasion of privacy, has shown a willingness to reconsider the privilege of confidentiality in a variety of areas, including health care[3] and the clergy-penitent privilege.[4]

Health care is a flashpoint for the debate over privacy because of the inherent sensitivity of our medical records. Used properly, medical records can be disclosed for life-saving purposes. Used improperly, the results can be very damaging to one's reputation or ability to seek employment. In the health

---

† Associate Professor, University of Michigan School of Public Health. I wish to thank Fouad Pervez, MPH, for excellent research assistance. I also wish to thank participants in the Privacy Symposium, both students and faculty, for insightful comments on these issues.

1. Polly Sprenger, *Sun on Privacy: "Get Over It,"* WIRED NEWS, Jan. 26, 1999, *at* http://www.wired.com/news/politics/0,1283,17538,00.html (quoting Scott McNealy).

2. *Id.*

3. *See, e.g.*, Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334, 350 (Cal. 1976).

4. Emily Eakin, *Secrets Confided to the Clergy Are Getting Harder to Keep*, N.Y. TIMES, Feb. 16, 2002, at A19.

care industry, the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[5] standards regulating privacy appear to counter McNealy's statement. On the surface, health information will be highly protected under the HIPAA regulations (known as the Privacy Rule) going into effect in 2003. HIPAA is intended to protect an individual's private medical records—known as protected health information (PHI) in the HIPAA regulations—from disclosure without the patient's written consent.[6] PHI is defined as individually identifiable health information electronically submitted or maintained by a covered entity.[7] Covered entities include all health care providers and health plans, along with business associates who receive PHI.[8]

As is common with complex federal legislation, the terms of engagement in HIPAA are amorphous and subject to a variety of interpretations. The proposals offered by Professors Larry Gostin and James Hodge offer a notable attempt to provide early guidance on how to interpret HIPAA for public health purposes. In this Article, I will respond to the Gostin and Hodge proposals and offer my own alternative approach to implementing the HIPAA regulations. Gostin and Hodge argue from a utilitarian perspective that the individual's private medical records should yield to communal public health needs when the benefits to public health are high and the risks to individuals are low.[9] That is fine in clear cases such as bioterrorism, but it is not clear from their presentation what the constraints would be in protecting individual privacy from a less compelling range of communal benefits. Still, there is much to admire in the Gostin and Hodge attempt to reconcile individual privacy with communal needs. As usual, they have provided an insightful and thoughtful analysis that is likely to generate additional commentary and responses.

In the end, however, I do not think they offer an approach that will be easy to implement. As an alternative, I suggest

5. Pub. L. No. 104-191, 110 Stat. 1936 (1996).

6. 45 C.F.R. § 164.501.

7. *See id.* (defining protected health information).

8. *See id.*

9. James Hodge, Presentation at the *Minnesota Law Review* Symposium: *Modern Studies in Privacy Law* (Feb. 9, 2002) (presenting Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439 (2002).

that we use a modified rule of reason approach to protecting the privacy of medical records, with the default option in favor of protecting privacy as opposed to disclosure. My premise is that privacy involves fundamental values that cannot easily be subjected to a utilitarian construct. Although a balancing test is an inevitable part of the privacy debate, protecting privacy is so fundamental to the health care enterprise that it should be viewed as being at or near the top of a hierarchy of values. Private information should be disclosed only under limited circumstances.

PRIVACY

An extended discussion of privacy is neither necessary nor appropriate for this Article. Nonetheless, a few words about it will help set the context for my subsequent remarks.

Privacy, an individual's claim to control personal health information, and confidentiality, an individual's ability to control disclosure of private information, are essential aspects of the clinical encounter. Privacy and confidentiality are at the heart of developing and maintaining trust in the physician-patient relationship.[10] Without a sense that privacy will be protected, the physician-patient relationship will suffer, to the detriment of patients.

At the same time, an individual's privacy right is not absolute and is certainly not the only value at stake in medical care and the use of medical records. Quality of care and cost containment are well-recognized public policy goals that need to be considered in deciding whether to disclose an individual's medical records. At issue is the tension between legitimate demands for the information and protecting privacy. Protecting privacy is not cost-free if doing so interferes with quality of care, especially continuity of care across health care providers, or impedes legitimate cost-containment efforts. While I place privacy above these competing policy goals in the hierarchy of values, the reality is that the competing policy objectives cannot be ignored.

Gostin and Hodge, therefore, are correct in framing the issue as a balancing arrangement. Indeed, the HIPAA statute

10. *See* Mark A. Hall et al., *Trust in Physicians and Medical Institutions: What Is It, Can It Be Measured, and Does It Matter?*, 79 MILBANK Q. 613, 622 (2001); David Mechanic, *The Functions and Limitations of Trust in the Provision of Medical Care*, 23 J. HEALTH POL. POL'Y & L. 661, 671-72 (1998).

and privacy regulations strongly suggest that Congress recognized the need to balance competing interests. As I will argue below, however, that balance must be carefully weighted toward protecting privacy. The primary reason for inserting a hierarchy of values into the equation is the serious adverse consequences of disclosing private data. A secondary reason is that disclosure is exacerbated by information technologies. In an era of paper-only records, disclosure could be embarrassing, but would usually be limited in scope. With the anticipated widespread adoption of digital medical records, that same disclosure can now be sent instantaneously to millions of unsuspecting recipients.[11]

Without much elaboration of each point, there are four major concerns about unwarranted disclosure of private health information. First, in the wrong hands, PHI can be used to discriminate against individuals in employment or insurance based on pre-existing health conditions or other health or social factors. Privacy advocates are particularly worried that information about potential genetic deficiencies will be used to deny employment or life insurance. To date, however, there are few reported instances of such discrimination.[12]

Second, releasing PHI can prove very embarrassing to the individual, even if there is minimal harm. For instance, it may have no discriminatory implications if I have been treated for a sexually transmitted disease or for depression, but public disclosure of this information could be embarrassing.

Third, there is little doubt that disclosing PHI will lead to a barrage of marketing from pharmaceutical manufacturers and other health care suppliers. To be sure, as I will discuss below, that information can be very useful, but it can also be unwanted and undesirable. As a patient, I may not want to be

11. Three anecdotes should suffice to make the point. First, a local public health official loaded a laptop with individually identifiable AIDS data. The laptop was stolen. Second, a former research assistant's boyfriend hit the wrong button on a cell phone, which resulted in unknowingly recording a long meeting on my assistant's voice mail. Imagine if the boyfriend had been engaged in an activity he would prefer not to disclose to my assistant! Third, Eli Lilly & Company disseminated (no doubt unintentionally) the e-mail addresses of some 600 patients taking their anti-depression drug Prozac. Robert O'Harrow, Jr., *Prozac Maker Reveals Patient E-mail Addresses,* WASH. POST, July 4, 2001, at E1.

12. For an interesting debate on this topic, see *When Genes Are Decoded, Who Should See the Results?*, N.Y. TIMES, Feb. 29, 2000, at F7; *see also* Paul Steven Miller, *Genetic Discrimination in the Workplace*, 26 J.L. MED. & ETHICS 189, 189 (1998).

reminded constantly about my illness, and the more lists my name is on, the greater the chances of an unwelcome disclosure. Because of these concerns, the marketing exemption to HIPAA's informed consent requirement has generated considerable opposition from both physicians and patient advocacy groups.[13]

Fourth, perhaps the most serious potential consequence of releasing PHI is to undermine a patient's trust in the entire health care system. From both an ethical and a legal perspective, patients expect confidentiality when dealing with medical professionals. The concept of fiduciary duty, the duty of loyalty a physician owes to the patient, is fundamental to the therapeutic encounter.[14] Violating this norm may have serious repercussions if patients begin to withhold information from their physicians for fear of having it disclosed to third persons.

In fairness, there are certain positive uses of PHI that should be considered. First, sharing PHI among medical professionals may be crucial for monitoring the quality of care and for maintaining continuity of care. For example, physicians and pharmacists must have accurate data on all pharmaceuticals a patient takes to prevent adverse drug-drug interactions. The American Hospital Association (AHA) argues that health professionals need a full picture of the patient's health, not a small amount of information about one specific condition, to avoid complications.[15]

The second positive use of PHI is to provide access to information for research and public health purposes. For research, such accessibility can be maintained by providing data

13. *See, e.g.*, Amy Snow Landa, *Physicians Protest Privacy Rule Loophole*, AM. MED. NEWS, Feb. 11, 2002 (arguing that "[t]he marketing provisions provide several exemptions that essentially 'swallow the rule' requiring patients' prior consent"), *available at* http://www.amednews.com.

14. *See, e.g.*, Peter D. Jacobson & Michael T. Cahill, *Fiduciary Responsibilities in the Managed Care Context*, 26 AM. J.L. & MED. 155, 157 (2000) (noting that "[t]he underlying justification for using the fiduciary model is that a patient's trust in his or her physician is the foundation of a morally acceptable health care system"); *see also* PETER D. JACOBSON, STRANGERS IN THE NIGHT: LAW AND MEDICINE IN THE MANAGED CARE ERA (forthcoming 2002) [hereinafter JACOBSON, STRANGERS IN THE NIGHT].

15. *See, e.g.*, AM. HOSP. ASS'N, STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION: OVERVIEW AND IDENTIFICATION OF KEY ISSUES SCOPE, *at* http://www.aha.org/ar/Advocacy/privacystandards99.asp (2002); Lawrence O. Gostin, *National Health Information Privacy: Regulations Under the Health Insurance Portability and Accountability Act*, 285 JAMA 3015 (2001).

that does not identify any individual patient. For public health, Gostin and Hodge make a persuasive case that at least under certain circumstances, individually identifiable information must be shared.[16] Indeed, as Peter Swire and Lauren Steinfeld also note,[17] HIPAA permits exceptions to privacy protections for national security,[18] as well as for research[19] and public health uses.[20]

Finally, PHI can be valuable for marketing directly to individuals. While the merits of direct-to-consumer pharmaceutical marketing are controversial, such marketing provides individuals with knowledge of products pertaining to their medical condition that might otherwise go unnoticed. Using PHI to provide marketers with access to specific conditions can thus have positive quality of care outcomes by alerting patients about new medications.

HIPAA

Since the overview of HIPAA and its accompanying regulations[21] is covered very nicely by Gostin and Hodge and others in this symposium, I will just briefly recount what I view as some of HIPAA's advantages and disadvantages. As a point of departure, HIPAA is beset by critics on all sides, but the statute does have certain strengths.

At least on its face, HIPAA provides strong privacy protection for PHI.[22] The extensive regulatory standards apply to all health care providers and health plans, and require them to protect PHI with their business partners.[23] To avoid heavy fines and penalties, covered entities will need to develop policies and procedures to protect PHI from unwarranted disclosure.[24] If properly implemented, HIPAA regulations will have the desirable effect of streamlining health information much

16. Hodge, *supra* note 9.

17. Peter P. Swire & Lauren Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515 (2002).

18. 45 C.F.R. § 165.512 (2001).

19. *Id.*

20. *Id.*

21. *See generally* 45 C.F.R. §§ 160.101-312, 164.500-34 (2001).

22. Insure.com, *The HIPAA law: Your rights to health insurance portability*, *at* http://www.insure.com/health/hipaa.html (Jan. 12, 2002).

23. David Hellerstein, *The Rules Are Out*, HEALTH MGMT. TECH., Feb. 2001, at 8, *available at* http://www.healthmgttech.com/cgi-bin/arttop.asp?Page=hipaa0201.htm.

24. *See* AM. HOSP. ASS'N, *supra* note 15.

more than previously seen. Data collection and transmission will be standardized to a large extent. Doing so will result in billing and transaction efficiencies, minimize systems errors in interpreting a patient's medical condition, and ease communication across the system. In turn, these efficiencies should result in lowering the administrative costs of health care.

One other conceptual advantage is that HIPAA may enhance communication between health professionals and patients. Because health professionals are forced to obtain consent from the patient before releasing PHI, physicians have an opportunity to discuss the nature of the patient's illness and the proposed therapeutic regimen.[25]

HIPAA's critics argue that its costs vastly outweigh its advantages. As noted earlier, there are legitimate concerns that HIPAA's restrictions will undermine the quality and continuity of care.[26] The Blue Cross Blue Shield Association believes that HIPAA standards will slow the delivery of payment and health care to patients, threatening both the quality of care and HIPAA's advantage in reducing health care costs.[27] More importantly, at least from the industry's perspective, is that HIPAA will be very costly to implement. The AHA claims that the government's cost estimates for implementing HIPAA are much lower than the real costs. According to the AHA, HIPAA will be much more expensive than originally expected, and that the two years given to the industry to implement the standards is not enough time.[28]

In addition to the sizeable costs associated with implementing HIPAA, the regulations are complex, detailed, and will be difficult to implement consistently. For one thing, they may well unintentionally conflict with other, equally detailed regu-

25. There are, of course, any number of reasons to be skeptical that this will occur, not the least of which is that physicians have not always been aggressive in seeking informed consent. *See, e.g.*, Peter D. Jacobson & C. John Rosenquist, *The Use of Low-Osmolar Contrast Agents: Technological Change and Defensive Medicine*, 21 J. HEALTH POL. POL'Y & L. 243, 259-60 (1996) (discussing the disappointing informed consent results in the context of their contrast injection study). This advantage could be jeopardized if the Department of Health and Human Services makes final its proposed rule to remove the consent requirement. *See* 67 Fed. Reg. 14,775 (Mar. 27, 2002).

26. *See supra* note 14 and accompanying text.

27. Am. Health Law. Ass'n, *Privacy Rule Will Force Major Changes in Handling of Patient Information*, HEALTH LAW. NEWS, Feb. 2001, at 5-6.

28. *See* AM. HOSP. ASS'N, IMPROVING PATIENT CARE AND REDUCING THE REGULATORY BURDEN, *at* www.aha.org/ar/Advocacy/informationsystems.asp. Of course, industry estimates have often been a bit exaggerated.

lations, such as the fraud and abuse regime. For another, the HIPAA regulations are so complex that they may simply collapse of their own weight. They are very difficult to follow, so that even well-intended health care administrators may be unable to decipher their meaning. HIPAA was supposed to create more efficiency, but in its current form it is likely to create more bureaucracy. Additional paperwork will be required, especially with numerous patient consent forms.[29] At this point, it is difficult to foresee how the Department of Health and Human Services (HHS) will be able to enforce the HIPAA regulations in any meaningful way.

Perhaps the most significant concern about HIPAA is whether its exemptions actually undermine its strong privacy protections. PHI is supposed to be safeguarded by HIPAA, but can still be used and accessed without authorization for payment or for health care operations. There is a lengthy list of instances in which PHI can be disclosed without the patient's consent.[30] More importantly, once a covered entity has the patient's informed consent, PHI can be easily disclosed to a variety of entities. In a sense, HIPAA giveth and then taketh away. As is well-known, most patients simply sign the forms that are presented without fully understanding their contents or implications. And HIPAA standards do not regulate PHI being sold by the covered entity to other companies for advertising and marketing purposes.[31]

HIPAA has become a major source of confusion with its countless standards. There are detailed protocols for health professionals regarding contracts and agreements of patient consent before using e-mail to communicate with them (although HHS has agreed to soften this position).[32] This appears to be quite excessive, especially considering that the use of e-mail would likely improve quality of care for the patients. Thus, a serious concern about the HIPAA regulations is whether the focus has shifted from broadly protecting privacy

29. *See* Jonathon S. Feld & Ryan D. Meade, *Trends Strong Medicine for Health Care Privacy Crimes*, 7 BUS. CRIMES L. REP. 1 (2000), *available at* LEXIS, News Group File, All.

30. 45 C.F.R. § 164.506 (2001); *see also* AM. HOSP. ASS'N, *supra* note 15.

31. Gostin, *supra* note 15, at 3019-20 ("A covered entity may use or disclose protected health information without the person's permission for marketing communications to that individual that occur in face-to-face encounters or concern products or services of nominal value.").

32. *Get Patient's Written Consent Before Using E-mail*, HEALTH INFO. COMPLIANCE INSIDER, Sample Issue, 2001, at 5-6.

to meeting detailed standards. In short, has privacy been lost in the thicket of a complicated regulatory structure? Have the HIPAA regulations done enough to protect privacy or have the exemptions overwhelmed what HIPAA was designed to protect? In July 2001, HHS was forced to issue a policy entitled Guidance on the Privacy Standards to clarify confusion over HIPAA's terms.[33] One of the major points in the Guidance is that covered entities are not required to guarantee the privacy of protected health information; they are required to only make "reasonable" efforts to protect the confidentiality and security of that information.[34] More ominously, HHS has proposed a new rule that would virtually eliminate the consent requirement. While covered entities would still be required to inform patients about their privacy rights, the entities would no longer need to obtain written consent before disclosing PHI. At this point, the proposed rule would apply only to uses and disclosures for treatment, payment and health care operations.[35] Nonetheless, it represents a departure from HIPAA's privacy protections and may presage further erosion of regulatory oversight.

A key concept in HIPAA's privacy rule is that covered entities are to "make reasonable efforts to limit [use or disclosure of] protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[36] Unfortunately, the elements of the "minimum necessary standards" are not defined in the current regulations,[37] and it has been difficult to generate agreement on how the concept should be implemented. This term is ambiguous and requires a significant effort to determine what is and is not necessary to tell other health professionals, since many factors

33. U.S. DEP'T OF HEALTH AND HUMAN SERVS. OFFICE FOR CIVIL RIGHTS, STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (45 C.F.R. pts. 160 and 164) (2001), *available at* http://www.hhs.gov/ocr/hipaa/finalmaster.html.

34. *See* Jon Nygaard & David Hoffmeister, *New HIPAA Privacy Regulations Clarified in Guidance*, 1 WSGR LIFE SCI. BULL. Issue 2 (2001), *at* www.wsgr.com/library/libfileshtm.asp?file=LSonline3.htm; Kristen Rosati, *The HIPAA Privacy Guidance: Preview of a "Reasonable" Enforcement Posture*, HEALTH L. DIG., Oct. 2001, at 3.

35. *See* 67 Fed. Reg. 14,775 (Mar. 27, 2002).

36. 45 C.F.R. § 164.502(b)(1).

37. *See* John R. Christiansen, *A Preliminary Review of the Final HIPAA Privacy Rule: Re-Engineering the Information Relationship Between Individuals and Healthcare Organizations*, HEALTH L. DIG., Feb. 2001, at 3-12.

come into play.[38]

OPTIONS

At the present time, it is impossible to determine whether the advantages or disadvantages of HIPAA will outweigh the other because the regulations do not go into effect until 2003. Nevertheless, it is worth considering options that might facilitate HIPAA's successful implementation and alternatives to replace HIPAA if it fails.

To facilitate implementation, Gostin and Hodge offer their balancing approach, heavily weighted toward communal interests.[39] I will have more to say about this in a moment. An alternative implementation strategy is to rely on a broadly defined "rule of reason" similar to HHS's recent Guidance.[40] I will also expand on this idea later. A third implementation approach is to simply allow the process to take place and make regulatory adjustments over time as needed. Fourth, HIPAA's data security provisions may offer ways of minimizing the extent of harm from any disclosure. For instance, the Connecticut Hospital Association has employed technology to comply with HIPAA, using digital signatures, identity cards, secure web and e-mail, and controlled access to medical records.[41] Through encryption and different forms of security, participants claim success in protecting PHI.[42]

Finally, instead of governmental oversight, one might rely on the private accreditation bodies (the Joint Commission on Accreditation of Healthcare Organizations and the National Committee on Quality Assurance) to oversee compliance. This has the advantage of giving the private sector a stake in successful implementation, but the disadvantage of the private sector's disappointing track record in similar endeavors.[43]

Suppose that implementation fails—what then? One option is to scrap the HIPAA regime and start all over. Given the conceptual and practical hurdles facing HIPAA, this is an entic-

38. *See id.* (failing to define the minimum necessary).

39. Gostin & Hodge, *supra* note 9.

40. *See supra* note 33 and accompanying text.

41. John T. Lynch & Bruno Lassus, *Mega Enterprise Chooses Smart Cards*, 21 HEALTH MGMT. TECH. 50, 50 (2001).

42. *See id.*

43. For a more detailed analysis, *see generally* Peter D. Jacobson, *Regulating Health Care: From Self-Regulation to Self-Regulation?*, 26 J. HEALTH POL. POL'Y & L. 1165 (2001).

ing option. Yet as Professor Swire points out, it is unrealistic to expect Congress to revisit the privacy issues.[44] Even if, though unlikely, Congress were to reconsider, there is no guarantee that the reconsideration would result in more stringent privacy protections.

A final option, offered by Minnesota Attorney General Mike Hatch, is to allow disputes over privacy disclosure to be resolved by common law rather than through regulation.[45] Implicit in this option is that the courts will actually protect privacy. But there is reason to be wary about how assiduously the common law will protect privacy. First, the courts will need to resolve health care privacy litigation in the context of competing social policy goals. As noted earlier, cost containment goals may conflict with protecting PHI. To date, judges have generally protected managed care's cost containment objectives against patient challenges.[46] Second, the case of *Doe v. Southeastern Pennsylvania Transportation Authority*[47] provides a specific warning in relying on common law. In *Doe*, the court held that an individual could not recover damages for breach of privacy when his AIDS status was improperly (though inadvertently) disclosed during a legitimate cost containment review.[48] The court resolved the policy conflict in favor of cost containment.[49] Third, courts are now less protective of confidential information gathered during physician peer review credentialing decisions.[50] While this trend is not directly applicable to PHI, it certainly suggests changes in judicial doctrine that do not necessarily favor privacy protection.

---

44. Peter P. Swire, Presentation at the *Minnesota Law Review* Symposium: *Modern Studies in Privacy Law* (Feb. 9, 2002) (presenting Peter P. Swire & Lauren B. Steinfeld, *Security and Privacy after September 11: The Health Care Example*, 86 MINN. L. REV. 1515 (2002)).

45. Minnesota Attorney General Mike Hatch, Presentation at the *Minnesota Law Review* Symposium: *Modern Studies in Privacy Law* (Feb. 9, 2002).

46. For a detailed analysis, see generally JACOBSON, STRANGERS IN THE NIGHT, *supra* note 14.

47. 72 F.3d 1133, 1142 (3d Cir. 1995) (citing Fraternal Order of Police, Lodge 5 v. Philadelphia, 812 F.2d 105, 113 (3d Cir. 1987)).

48. *Id.* at 1143.

49. *Id.*

50. *See, e.g.*, Pa. Prot. & Advocacy, Inc. v. Houstoun, 228 F.3d 423, 428-29 (3d Cir. 2000); Virmani v. Presbyterian Health Servs. Corp., 515 S.E.2d 675, 697 (N.C. 1999), *cert. denied*, 529 U.S. 1033 (2000); *see also* State *ex rel.* Tennill v. Roper, 965 S.W.2d 945, 948-49 (Mo. Ct. App. 1998) (ordering discovery on the ground that the entity in question did not qualify as a "peer review committee" under state law).

COMMENTS ON THE GOSTIN AND HODGE APPROACH

Professors Gostin and Hodge are to be commended for offering a strategy that explicitly recognizes the public health community's interest in and need for certain PHI when that information would affect public health. There is no question that public health could not function in a world of absolute protection of individual health information. Thus, the real strength of their proposal is that it creatively shifts the discussion away from privacy to communal interests without excessively burdening individual interests. This approach also carves out a public health niche within HIPAA where we might think differently about how to strike the balance inherent in protecting the privacy of individual medical records. As such, it is a feasible alternative on conceptual, practical, and political grounds.

As a conceptual matter, their broad standard is entirely defensible: Where the potential public benefits are high and the risk of harms to individuals are low, PHI can be disclosed for important public purposes.[51] The test is most attractive on conceptual grounds because it provides a very useful analytical framework. Over a range of cases applying this standard, covered entities will develop rules and heuristics to guide subsequent decisions. It also provides an excellent starting point for thinking generally about public health problems, such as requiring motorcycle riders to wear helmets, where the intrusion into individual rights must be balanced against the state's interest in protecting the public's health, welfare, and safety.[52]

Another advantage of the Gostin and Hodge analysis is that it works within the HIPAA framework, hence avoiding the need to reconsider HIPAA. HIPAA contains an explicit exemption for public health concerns,[53] though the regulations do not provide guidance on how to define the exemption. By elaborating on HIPAA's existing provisions, Gostin and Hodge provide a mechanism for analyzing the balance in ways that will enhance and give meaning to HIPAA's structure and somewhat ambiguous terms. Anchoring their analysis in HIPAA provides clear conceptual limits to when the community's interests outweigh

51. For a widely cited framework for analyzing legislation and regulation that share some of these same attributes, see James Q. Wilson, *The Politics of Regulation, in* THE POLITICS OF REGULATION (James Q. Wilson ed., 1980).

52. For an extensive analysis of how Professors Gostin and Hodge might weigh the balance unconstrained by HIPAA, see LAWRENCE O. GOSTIN, PUBLIC HEALTH LAW: POWER, DUTY, RESTRAINT (2000) (especially Chapter 4).

53. 45 C.F.R § 164.512 (2001).

those of the individual.

But their approach has several significant disadvantages as well. Probably the most important concern is that Gostin and Hodge do not set forth clear criteria for how they would determine risks and benefits. Although their approach is conceptually sound, the problem comes in trying to operationalize the standard. How are we to define and weigh the public benefits and private risks?[54] To be sure, policymakers weigh such incommensurate values all the time. Yet even a cursory look at the literature suggests considerable dissatisfaction with current methodologies for doing so and widespread disagreement over the results. One need only look to environmental policy for repeated examples of this problem.[55]

In certain cases, specifically bioterrorism, the risk-benefit calculation is likely to be generally straightforward and uncontroversial. Most people will likely agree that some individual rights must yield to protect the community's right to contain a bioterrorism outbreak.[56] What about less obvious issues such as data obtained through needle-sharing programs, the spread of drug-resistant strains of tuberculosis, mandatory reporting of neonatal AIDS status by name, or cancer registries? How are we to weigh the risk-benefit ratio in those cases? The public benefits are high, but the risk of harm to individuals is not negligible—a situation more likely to be the norm than the bioterrorism example. Would the Gostin and Hodge framework support disclosure of PHI in these instances? It is hard to tell from their analysis, but their default option seems to be in favor of communal use and disclosure. In this sense, their schema is susceptible of being overly inclusive of situations that would permit disclosure. Before endorsing their model, I would like to see how it would apply in some of the more diffi-

54. *See* Peter D. Jacobson & Matthew L. Kanna, *Cost-Effectiveness Analysis in the Courts: Recent Trends and Future Prospects*, 26 J. HEALTH POL. POL'Y & L. 291 (2001) (outlining the difficulties in assigning such values in the context of managed care organizations' cost-effectiveness analyses).

55. *See generally* Competitive Enter. Inst. v. NHTSA, 45 F.3d 481 (D.C. Cir. 1995); Competitive Enter. Inst. v. NHTSA, 956 F.2d 321 (D.C. Cir. 1992); Corrosion Proof Fittings v. EPA, 947 F.2d 1201 (5th Cir. 1991); Cass R. Sunstein, *Health-Health Tradeoffs*, 63 U. CHI. L. REV. 1533 (1996).

56. *Cf.* George J. Annas, *Bioterrorism, Public Health, and Civil Liberties*, 346 NEW ENG. J. MED. 1337 (2002). As a caveat, however, note the rising incidence of adults who refuse to allow their children to be vaccinated for fear of autism. IMMUNIZATION SAFETY REVIEW COMM., INST. OF MED., IMMUNIZATION SAFETY REVIEW: MEASLES-MUMPS-RUBELLA VACCINE AND AUTISM 52-53 (Kathleen Stratton et al. eds., 2001).

cult situations likely to occur.

Aside from definitional concerns, Professor Ted Janger raised some additional issues during the Symposium that any standard that imposes a balancing test must meet. These include determining who the decision-maker will be; the timing of the decision (i.e., an *ex ante* or *ex post* balancing); who will have the burden of proof; how will that burden be met; and what the remedy will be for an improper disclosure.[57] Of these, the elements that Professors Gostin and Hodge most need to specify are who will make the balancing determination, who has the burden of proof, and what evidence will satisfy that burden. Without more details on how their standard will be operationalized along these dimensions, it is difficult to assess how well it might work in practice.

Finally, it seems unlikely that this model could be easily applied to the private health sector, which is the crux of HIPAA. Arguably, one might apply something akin to the second part of the Gostin and Hodge standard to PHI: Where public benefits are negligible and the risks of harms to individuals are high, privacy should restrict disclosure.[58] The problem is that the likely disputes will not be over public benefits. Instead, the dispute will be whether PHI is needed for legitimate quality of care concerns. Even if we were to substitute the phrase "legitimate clinical benefits" for public benefits, the standard is unlikely to be satisfactory. I will discuss the reasons why in a moment.

In sum, for the narrow exception of specific public health concerns, the Gostin and Hodge approach makes sense and should be followed. But as a statement of broad applicability to the entirety of HIPAA, I doubt that their strategy is workable.

AN ALTERNATIVE: A MODIFIED RULE OF REASON ANALYSIS

Assuming that the HIPAA regime will remain in place, and assuming that my concerns about using the Gostin and Hodge model broadly to PHI are legitimate, what approach might facilitate successful implementation? My alternative strategy is

57. Professor Ted Janger, Presentation at the *Minnesota Law Review* Symposium: *Modern Studies in Privacy Law* (Feb. 9, 2002) (presenting Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. ____ (2002)).

58. Gostin & Hodge, *supra* note 9.

analogous to the HHS Guidance, which attempted to bring order to the initial regulations, and to the rule of reason analysis in antitrust policy.

As a starting point, it is important to recognize the constitutional standard that people are entitled to a reasonable expectation of privacy.[59] Since the right to privacy is not an absolute, any schema must make room for times when privacy must yield to other competing public policy objectives. Therefore, as with the Gostin and Hodge model, some balancing is necessary. Where my approach departs from theirs is in relying more on a hierarchy of values, with protecting private medical records as a preeminent value. The standard I propose is a modified version of the rule of reason.

As with Gostin and Hodge, I anchor my analysis in the HIPAA framework, building on HIPAA's minimum necessary standard. As noted earlier, this standard requires covered entities to determine who has access to PHI, but does not set forth criteria for covered entities to make that decision.[60] At the present time, there is no agreement on what this provision means. It is beyond the scope of this Article to define the standard in detail, but in brief it would be to focus the definition around three concepts.

First, my default option favors privacy. As a matter of social policy and constitutional protection, privacy is a fundamental value to be protected. As a matter of first principles, patients have the right to expect that their medical records will only be viewed by those with a need to know. Even if privacy is not an absolute right, placing privacy above competing public policy goals, especially when the issue is private medical records, reflects the social value the public attaches to "being left alone." For this reason, medical professional ethical obligations place a high value on physician-patient confidentiality. A patient's privacy should be overruled cautiously and only with a strong showing of a need to disclose. As such, this default option goes beyond the reasonableness standard emerging in the HHS Guidance.

Second, the basis of the need to know standard (i.e., the

59. *See* Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring) (noting that a reasonable expectation of privacy exists with respect to such areas as a home or an enclosed telephone booth, where a person subjectively expects privacy, and society recognizes that expectation as reasonable).

60. *See supra* notes 37-38 and accompanying text.

minimum necessary) should be a determination of what is in the patient's best interests. Decisions to disclose PHI should focus on the patient's clinical needs and the legitimate need for sharing data to maintain continuity and quality of care. The burden should be placed on the entity that wants access to PHI to demonstrate the need for the information and that the request is narrowly tailored to meet that need.[61] Before releasing PHI, the covered entity must develop and implement policies and procedures that will meet or exceed the minimum necessary test. One way to meet the burden will be to demonstrate that the nature of the patient's illness requires treatment by several medical professionals or that sharing the information is crucial to prevent adverse clinical outcomes, such as drug-drug interactions.

Third, covered entities should be held to a reasonableness test, with the privacy default as the guide to what constitutes reasonable need for the information. The HHS Guidance appears to have adopted an operational test grounded in reasonableness. The rule of reason analogy becomes applicable here.[62] In a rule of reason analysis in the antitrust arena, courts balance the pro- and anti-competitive gains of a transaction, such as a merger, that raises antitrust concerns. In deciding whether to release medical records, the covered entity needs to make a good faith effort to explain why the PHI is needed. Thus, for example, it is not reasonable to prevent a pharmacist from filling a prescription when phoned in by a physician in the absence of a patient's written consent. Nor is it reasonable to impede using PHI for inpatient admissions or treatment scheduling without signed consent. A reasonableness standard will also protect common hospital practices such as sign-up sheets and maintaining patient medical records on bedside charts.[63] What is reasonable must be tempered by taking into account the dominant privacy value.

Another reason for using reasonableness as a criterion is that compliance will most likely be based on a good faith test.

---

61. This is a familiar constitutional standard. *See* GOSTIN, *supra* note 52, at 77-81 (outlining the levels of constitutional review of public health activities).

62. *See, e.g.*, NCAA v. Board of Regents, 468 U.S. 85 (1984); Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679 (1978).

63. *See* Rosati, *supra* note 34, at 3-11 (describing health care organizations' fear that the privacy standards would force discontinuation of some common healthcare practices).

In reality, as long as a covered entity puts in place a compliance program, the government is not likely to levy severe sanctions. The government routinely settles for a fraction of the possible penalties in fraud and abuse cases when the facility has implemented a good faith compliance effort.[64] There is no apparent reason why the same would not apply to HIPAA.

One might argue that my alternative is really nothing more than the inverse of the Gostin and Hodge framework, with my default option being to protect privacy and their default being to protect the community. To a certain extent, that would be an accurate observation. In particular, if we were only talking in HIPAA about public health, I would be inclined to work within their framework. At heart, though, we are operating on different conceptual models when we move to private medical records. Where the Gostin and Hodge model is avowedly utilitarian, my approach is much more deontological in recognizing a hierarchy of values.

A second objection is that the privacy default will be undermined by HIPAA's informed consent standard. Under that standard, PHI can be shared if the patient consents. As we all know, most patients simply sign the forms provided without much opportunity for discussion or reflection. Most patients will not have a clue about the implications of informed consent for sharing PHI. As a result, informed consent standing alone is necessary but not sufficient to justify disclosure. The covered entity would still need to justify the disclosure based on the above standard.

IS IT TOO LATE TO PROTECT PRIVACY?

Is it too late to protect privacy? No, but I am dubious that we will be able to simultaneously safeguard privacy and allow appropriate access to medical records to maintain quality of care. Advances in technology, medical record-keeping entry, and the way medicine will be practiced in coming years all suggest continuing pressure to subordinate privacy to other policy goals. To take just one example, telemedicine (the use of technology to share clinical data across geographic boundaries) has the potential for soaring medical advances. It also has the potential to disseminate private health information widely across

64. *See* Michael A. Dowell, *Legal Audits and Investigations: A Key Component of Healthcare Corporate Compliance Programs*, 32 J. HEALTH L. 229, 230 (1999).

the internet.

We live in a different age now, one in which information is freely collected and disseminated. That makes it very difficult to protect privacy in ways that were possible in previous eras. A cost of the computer and technology age may be that our privacy cannot be as safeguarded as it once was. Perhaps, then, McNealy was right with his assertion that privacy is lost.[65] Something has indeed changed, and we must be willing to accept that when trying to implement (or perhaps reform) HIPAA.

On balance, I want the medical advances to continue, but I suspect that the public will balk at them if the cost of medical advances is a substantial diminution in privacy. Therefore, I favor a regime that still places privacy at the top of the hierarchy. Medical advances and protecting health information are not mutually exclusive.

Professors Gostin and Hodge are correct to insist that the public's health not be sacrificed to excessive fears of disclosing private health information. An absolute right to privacy is unattainable and perhaps even socially undesirable. Nevertheless, Attorney General Hatch makes a powerful case that in the end, it will be more costly to abandon stringent privacy protections than it will be to think of privacy as *primus inter pares*.[66] I am not yet ready to get over losing the ability to protect my privacy. Where there exists a compelling need to disclose PHI, fine with me. But the burden should not be on me to show why my privacy should be protected.

65. *See supra* note 1 and accompanying text.

66. Hatch, *supra* note 45.