Privacy As An Enabler, Not An Impediment: Building Trust Into Health Information Exchange

The new e-health environment calls for nuanced approaches to individual consent, with appropriate enforcement mechanisms.

by Deven McGraw, James X. Dempsey, Leslie Harris, and Janlori Goldman

ABSTRACT: Building privacy and security protections into health information technology systems will bolster trust in such systems and promote their adoption. The privacy issue, too long seen as a barrier to electronic health information exchange, can be resolved through a comprehensive framework that implements core privacy principles, adopts trusted network design characteristics, and establishes oversight and accountability mechanisms. The public policy challenges of implementing this framework in a complex and evolving environment will require improvements to existing law, new rules for entities outside the traditional health care sector, a more nuanced approach to the role of consent, and stronger enforcement mechanisms. [*Health Affairs* 28, no. 2 (2009): 416–427; 10.1377/hlthaff.28.2.416]

HEALTH INFORMATION TECHNOLOGY (IT) and electronic health information exchange (HIE) are critical tools for transforming our health care system. Policymakers are pushing initiatives to bring health care into the digital age. However, with rare exception, national efforts to advance health IT have not adequately addressed privacy. The debate about privacy has often seemed too polarized to resolve, gridlocking initiatives to promote health IT.

Although some persist in positioning privacy as an obstacle to achieving the advances that greater use of health IT may bring, we argue that the opposite is true: enhanced privacy and security built into health IT systems will bolster the public

Deven McGraw is director, Health Privacy Project, at the Center for Democracy and Technology (CDT) in Washington, D.C. James Dempsey (jdempsey@cdt.org) is vice president for public policy at the CDT in San Francisco. Leslie Harris is president and chief executive officer at the CDT in Washington, D.C. Janlori Goldman is on the faculty of the Center for the History and Ethics of Public Health, Department of Sociomedical Sciences, at the Columbia University School of Public Health in New York City.

DOI 10.1377/hlthaff.28.2.416

trust and confidence that are critical to the rapid adoption of health IT and realization of its benefits. There is a path forward to a second generation of privacy and security policies and technological solutions that build on existing law while responding to the new challenges of the e-health environment.

A large majority of the public wants electronic access to their personal health information, for themselves and their health care providers, because they believe that such access is likely to improve the quality of their care.[1] However, people also have major concerns about the privacy of electronic medical records (EMRs). In a 2006 national survey, 80 percent reported being very concerned about identity theft or fraud, 77 percent were very concerned about use of their medical information for marketing purposes, 56 percent worried that employers would access their health information, and 55 percent were concerned about insurers' seeing their data.[2]

The computerization of personal health information undeniably poses risks to privacy. Tens of thousands of health records may be accessed or disclosed through a single breach. Recent headlines about the theft of laptop computers containing unencrypted health information and inappropriate access to celebrities' records validate the concerns reflected in the survey data.

It is important to respond to these very real privacy and security risks, not just to build trust and avoid individual embarrassment or discrimination, but also because good health care depends on accurate and reliable information.[3] Without privacy and security assurances, patients will withhold information from their providers to avoid having it used inappropriately. One in six adults (17 percent)—thirty-eight million people—say that they engage in such "privacy-protective" behavior.[4] People with chronic illnesses and racial and ethnic minorities report even higher levels of concern about the privacy of their medical records and are more likely than average to withhold information for fear of its being improperly used.[5]

Building A Comprehensive Privacy And Security Framework

To build public trust in health IT, we need a comprehensive, second-generation privacy and security framework that sets clear rules for access to, use of, and disclosure of personal health information for all entities engaged in e-health and that includes adequate oversight and accountability. The Markle Foundation's multistakeholder Connecting for Health initiative has developed such a framework, structured around three key elements: implement core privacy principles; adopt trusted network design characteristics; and establish oversight and accountability mechanisms.[6]

The Connecting for Health framework is based on "fair information practices," a set of principles that have been relied on to define information privacy rights in a variety of contexts in the United States and internationally.[7]

■ **Policy challenge of HIPAA.** However, implementing this comprehensive framework of privacy protections for the complex and evolving e-health environ-

ment poses major policy challenges. These challenges start with the reality of the privacy regulations enacted pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

The HIPAA rules were a landmark in health privacy protection. To a limited extent, they embody some of the fair information practices in the comprehensive framework. However, the HIPAA regulations are inadequate even for the traditional health care sector. These weaknesses have grown more important as IT use and business practices in the traditional health care environment have evolved.

Meanwhile, HIPAA does not even apply to the entities from outside the health care sector that are now handling health information through new services such as personal health records (PHRs). Even a strengthened HIPAA Privacy Rule would not be well suited to these new entrants; they will probably require a different implementation of the comprehensive framework. The privacy principles in the framework are broad enough to work across platforms and business models, but applying them so as not to discourage innovation or favor one model over others will take considerable care.

■ **Implementation challenges.** In this complex environment, two implementation challenges stand out. One involves the role of consent (what HIPAA calls "authorization"). Some see consent as the linchpin of privacy, but in our view, consent requires special attention lest it be used to override all other protections, thereby weakening privacy. Second, enforcement needs to be improved across the board, although here, too, there is no silver bullet.

Therefore, to ensure that all entities that collect, store, or manage personal health information comply with baseline health information protections, policymakers will have to (1) strengthen HIPAA for records kept by or exchanged among traditional health system participants; (2) enact new legal protections that address the increased migration of personal health information out of the traditional health care system; (3) clarify the role of consent; and (4) develop more-effective enforcement mechanisms.

Strengthening HIPAA For The Traditional Health Care System

Strands of the fair information practices can be found in HIPAA, but some of the principles are only weakly expressed, and others are missing entirely. Making HIPAA a truly effective privacy law will require filling gaps, narrowing exceptions, and clarifying key terms.

■ **Coverage of RHIOs and HIEs.** State and regional health information organizations (RHIOs) or health information exchanges typically aggregate and facilitate the exchange of personal health information among providers and often between providers and health plans. However, they are not "covered entities" under HIPAA regulations.[8] Thus, it is not clear that they must enter into business associate agreements to exchange protected health information. It could be argued that these exchanges need a separate regime, but we conclude that they are so interwoven with

participants in the traditional health care system that it would be best to address them within the HIPAA framework. These new exchanges could be required to comply with HIPAA rules as either covered entities or business associates, depending on their structure and functions. For example, exchanges that merely facilitate the exchange of data among covered entities could be regulated as business associates for those activities; exchanges that collect and store data or have independent rights with respect to the data they hold could be covered entities.

■ **Marketing.** A core privacy principle is the limitation on secondary uses—uses beyond those for which the information was initially collected. Marketing is a secondary use, and survey data show that use of personal health information for marketing purposes without individual authorization is a key privacy concern. However, the definition of *marketing* in the HIPAA Privacy Rule far too often permits the use of protected health information without a patient's authorization to send that patient marketing materials regarding certain health care products or services. The deficiencies in the current rule will likely be exacerbated by the greater access to data facilitated by electronic exchange and the need for these nascent exchanges to find a viable business model to sustain start-up and long-term expenses—a business model that might come to include advertising.[9] We need tighter restrictions on marketing to increase the assurance that people's personal information cannot be used without their authorization to market goods and services to them.

■ **Deidentification.** HIPAA's protections do not extend to "deidentified" health information. Thus, covered entities may provide deidentified data to third parties for uses such as research and business intelligence without regard to HIPAA. In turn, these entities may use these data as they wish, subject only to the terms of any applicable contractual provisions (or state laws that might apply). If a third party then reidentifies these data—for example, by using information in its possession or available in a public database—the reidentified personal health information would not be subject to HIPAA.[10] It could be used for any purpose unless the entity holding the reidentified data was a covered entity.

A number of researchers have documented how easy it is to reidentify deidentified data.[11] The U.S. Department of Health and Human Services (HHS) should revisit the current deidentification standard in the Privacy Rule (in particular, the so-called safe harbor that deems data to be deidentified if they are stripped of particular data points), to ensure that it continues to present minimal risk of reidentification. At the same time, HHS and Congress should work together to ensure that recipients of these anonymized data are accountable if the information is reidentified.

■ **Health care operations.** The HIPAA Privacy Rule allows covered entities to use identifiable health information for a broad range of "health care operations" without the need to first obtain patient consent. Although covered entities need to be able to use health data for core health care operations, the list of uses in health care operations is overly broad. Covered entities are required to use only the mini-

mum necessary amount of data for health care operations.[12] However, this requirement refers to limits on the amount of data accessed or disclosed, not to the amount of identifying information that accompanies the data.[13] HHS should reexamine the health care operations exception; it might find that a number of the activities now included in operations could be performed with data stripped of common patient identifiers (for example, peer review activities and internal quality assessment), while others should be permitted only with authorization by patients.[14]

■ **Electronic access by consumers.** The HIPAA Privacy Rule provides individuals with access to their medical records, including the right to receive a copy "in the form or format requested," if those records are "readily producible" in that format.[15] However, the access right in the HIPAA rule is not being implemented very well. The failure to provide patients with their medical records—even in paper format—is one of the top five HIPAA complaints investigated by HHS.[16] In addition, the Privacy Rule allows covered entities to charge a "reasonable cost" for copying a patient's record, which reportedly range from free to $37 for up to ten pages.[17] HHS should issue guidance or modify the regulation to ensure that people can promptly obtain electronic copies of their health information whenever the data are stored in electronic form, for free or at a cost that appropriately reflects the ease of providing the record in electronic format.

Protecting Privacy When Personal Health Data Leave The Health Care System

PHRs and other services that enable consumers to store and manage their own or their family's health information are now being created by third parties, including Google, Microsoft, and WebMD, and by employers. Personal health data also are migrating onto the Internet through an exploding array of health information sites, support groups, and other online health tools. These tools and services, which appeal directly to consumers, fall outside of HIPAA unless they are being offered by covered entities. Where HIPAA does not apply, privacy is dependent on other existing mechanisms, including any applicable state health privacy or consumer protection law; the terms of the PHR's published privacy policy, if any; and market forces. Separately and together, these are inadequate.

Although the states have an important role to play in privacy policy, state privacy laws are fragmentary and inconsistent, providing neither developers nor consumers with the assurances they deserve, especially for services of nationwide reach. Privacy policies have their limits as well: if a promise made in a PHR privacy policy is routinely violated, the Federal Trade Commission (FTC) may bring an action against a company for engaging in a "deceptive trade practice," but nothing in federal law requires PHRs to state any privacy commitments in the first place. FTC actions on data security have been quite limited.

It has been suggested that the federal Electronic Communications Privacy Act (ECPA) of 1986 provides adequate protection for PHRs.[18] However, the relevant

"Relying on consent alone would provide very weak privacy protection, for consent is far too easy to obtain."

ECPA provision applies only to services that are offered to the public.[19] PHRs available exclusively to employees of a particular company, for example, fall outside of this part of ECPA. Moreover, ECPA applies only if the provider is not authorized to access the contents of a customer's records for purposes of providing any services other than storage or computer processing.[20] This caveat may knock out a lot of PHRs that provide services beyond data storage, or that are based on advertising and analyze individual patient records to target ads.

■ **Toughen consent.** In any case, both ECPA and most privacy laws of general applicability have exceptions for consent. For all the reasons we discuss below, relying on consent alone would provide very weak privacy protection for information in PHRs, for consent is far too easy to obtain. Although it is important that consumers have full, opt-in control over the information in their PHRs, a requirement to obtain consumer consent (either in existing law or a new mandate) could be implemented in such a way that most individuals would consent to very broad uses and disavow any other expectations of privacy. As explained in more detail below, consent forms are written by the entity seeking the data and are often worded in general or vague terms so that they cover all potential uses of the data. Consequently, consumers may inadvertently authorize uses of their health information via a consent form or policy that they do not fully understand. There is a crucial role for strong patient consent with respect to information in PHRs, but this consent should be situated within a clear framework of rules ensuring that consent is meaningful. For example, to ensure that consumers do not inadvertently grant blanket authorization for use of their data, regulators may have to address the form and content of the terms of service and the privacy policies for systems offering PHR services. The foundation of PHRs should be opt-in (that is, affirmative as opposed to implied consent), but even opt-in consent can be too general. Therefore, baseline regulatory standards might specify particular uses or disclosures for which independent consent must be obtained. For example, it might be required that consent to disclose data for marketing or commercial purposes must be obtained independently of other consent. Special consent might also be required for research uses of data, even if the data are deidentified or aggregated.

■ **Add prohibitions.** Policymakers may find it necessary to go further and prohibit certain uses or disclosures of data in PHRs, regardless of consent. Compelled disclosures pose a particular problem in the contexts of employment, credit, or insurance, where people are often compelled to sign authorizations granting employers, banks, insurers, and others access to their health records for nonmedical purposes. Although the problem of these disclosures, which are nominally voluntary but are in fact compelled, applies to traditional health records, it is exacerbated with

PHRs, which may contain not only copies of provider records but also user-generated data not revealed even to a doctor. If PHRs are to be encouraged, the best course may be to prohibit their use in the context of employment, credit, or insurance. Congress has already moved in this direction with the Genetic Information Nondiscrimination Act (GINA) of 2008, which prohibits employers from using genetic information to make employment decisions and prohibits health insurers from using such information to make coverage and underwriting determinations.[21]

■ **Include limits on data recipients.** A comprehensive privacy framework would also include limits on downstream recipients of data from PHRs. The revenue model to support many Internet-based PHRs will be partnerships with third parties who will offer services or "applications" to PHR account holders, which means that a consumer's PHR data may go to many organizations. Contractual agreements will be necessary to bind business partners to particular privacy and security policies, such as a commitment not to redisclose the data or to use them for purposes other than those for which consent was granted. However, such contractual commitments will be insufficient to build consumers' trust in PHRs. Even if such contracts were required to contain certain elements, consumers could not be assured of consistent enforcement.

■ **Define a floor of privacy protection.** Finally, some argue that the market is already driving toward models that offer consumers full control over the information in their PHRs. Although that is the direction of the market today, the market is very new and has only recently begun to evolve in this direction.[22] Consumers' interest in these tools is still low.[23] Because the data in PHRs are of high commercial value, there may be economic pressures on PHR providers to make use of data they hold—a prospect that becomes even more tempting if the current business model that supports full consumer control does not generate sufficient revenue. Instead of waiting to see where the market leads, policymakers should act to define a floor of privacy protection, upon which innovation can improve but below which none should be permitted to fall.

■ **Develop privacy rules for PHRs.** To achieve a consistent baseline of privacy protection, some have suggested extending the HIPAA Privacy Rule to cover PHRs. We believe that the rule, which was designed for traditional health care entities, would not provide adequate protection for PHRs and may do more harm than good in its current scope. Further, it might not be appropriate for HHS, which has no experience regulating entities outside of the health care arena, to take the lead in enforcing consumer rights and protections with respect to PHRs.

Instead, Congress should task HHS and the FTC with jointly developing privacy and security requirements for PHRs. For PHRs offered by entities that are not part of the traditional health care system, it is critical that regulators understand the business model behind these products, which will largely rely on ad revenue and partnerships with third-party suppliers of health-related products and services. The FTC seems to be the agency best suited for this kind of rule making.

However policy responsibility for PHRs is allocated, policymakers and the private sector need not start from scratch. Markle's Connecting for Health initiative last year released a "Common Framework for Networked Personal Health Information" that sets forth practices to protect personal information and increase individual participation in online PHRs.[24] This framework, developed through a multistakeholder, public-private collaboration and endorsed by major PHR vendors and leading consumer groups, could guide both governmental policies and industry best practices.

The Appropriate Role Of Consent

To an unfortunate degree, policy discussions about how best to protect the privacy and security of health information have been narrowly focused on the issue of individual consent. To many privacy advocates, patients' authorization of all uses of their personal health information is the essence of privacy.[25] To be sure, the ability to exercise control over one's own personal health information is an important element of privacy protection, and a comprehensive privacy framework should set out circumstances in which patients' consent must be obtained.

■ **Vagaries of consent.** However, consent is not a panacea. In practice, overreliance on consent would provide very weak protection. Unfortunately, most people do not focus on the details of consent forms, and many who do often do not understand the terms.[26] Many wrongly assume that the existence of a "privacy policy" means that their personal information will not be shared, even when the policy says just the opposite.[27] Consent forms are drafted by entities seeking to obtain and use health information. Their purpose is to authorize all of the entity's potential uses of the data, so most are phrased in ways intended to obtain consent.[28]

Moreover, people are normally asked to consent to use of their personal health information in circumstances where they are most likely to feel compelled to give it, when waiting to see a doctor or when applying for health insurance. It is unlikely that a person will say no if treatment or coverage can be denied on that basis or if a wide range of uses is covered under a single consent. The limits of consent were well illustrated by news accounts last year about health and life insurers' obtaining personally identifiable prescription drug records from third-party data miners. The companies that mine these data relied on individual consent to obtain sensitive prescription drug histories—consent that these people provided as a condition of applying for insurance.[29]

■ **Beyond consent.** Rules going beyond consent will be needed because there are some uses that should not be permitted even with consent. GINA provides an example of how rules are sometimes needed that provide stronger protection than consent alone. With these rules in place, people cannot be asked for permission to use their genetic information for employment or insurance purposes, because such uses are outright prohibited.

In other circumstances, it will be appropriate to require very specific consent

("authorization"). For example, a number of state laws already require patient authorization to access certain sensitive categories of health information, and federal law prohibits disclosure of substance abuse treatment records without express patient authorization.[30] Any such consent requirements should be in addition to clear rules that limit how the information can be accessed, used, and disclosed and that are adequately enforced. Further, better rules about how consent is obtained will help prevent people from inadvertently authorizing inappropriate uses of their health information.[31]

Policymakers should give special consideration to additional roles for consent in the new e-health environment, such as by giving patients the right to opt into or at least opt out of having their health information accessible through an exchange, or by strengthening a person's right to restrict access to particularly sensitive information.[32] Electronic health information systems must be structured in a way that allows these consents to be meaningfully presented to users and be honored by all system participants.

All in all, the new e-health environment calls for a much more nuanced approach to consent than the polarized privacy debate has yielded thus far.

Oversight And Accountability

When Congress enacted HIPAA in 1996, it included civil and criminal penalties for noncompliance, but those rules have never been adequately enforced.[33] As of November 2008, HHS had not levied a single penalty against a HIPAA covered entity in the nearly five years since the rules were implemented, even though that office has found numerous violations.[34] Further, a 2005 opinion from the Department of Justice (DOJ) Office of Legal Counsel expressly limited the application of the criminal provisions to covered entities. Although the DOJ has prosecuted individuals for criminal HIPAA violations in at least two instances since this opinion, its release had a chilling effect on enforcement of the criminal provisions.[35]

Also, under current rules, business associates who obtain, use, and disclose protected health information on behalf of covered entities are accountable for complying with HIPAA regulations only through their contracts with these entities. If the covered entity does not take action to enforce the contract, there is no other mechanism for ensuring that the business associate complies with applicable rules. HHS can hold the covered entity responsible for the actions of its business associates only if the entity knew of a "pattern of activity or practice of the business associate that constituted a material breach or violation" of its agreement with the covered entity and took no action in response.[36] This approach provides no incentive for covered entities to monitor whether their business associates are abiding by the HIPAA rules; rather, it ensures that downstream users of protected health information are out of reach of federal regulators.

The current rules arguably give HHS sufficient authority to aggressively and effectively enforce the law against covered entities, while also allowing room for the

agency to negotiate nonpunitive responses with entities whose HIPAA violations are minor. Overall, it is within the power of the new administration to implement an enforcement policy that is robust without making covered entities so overly cautious that they fail to share information even for those purposes where it is permissible and facilitates the provision of good care.

However, there are areas where action by Congress is needed, or where clarification of current law could improve enforcement. For example, Congress should act to make sure business associates are fully accountable for complying with the HIPAA regulations that are appropriate, given the scope of their contractual activities. As noted above, Congress should also enact prohibitions and penalties for the unauthorized reidentification of deidentified data. In addition, Congress could make it clearer that HHS must pursue civil monetary penalties for HIPAA violations involving willful neglect.

It may be necessary to develop enforcement mechanisms specifically tailored to PHRs. We suggested above that the FTC have a role in developing rules for PHRs, applying its expertise in consumer protection. The FTC would also need appropriate power to enforce such rules, which it could apply in addition to its existing authority over unfair and deceptive trade practices.

To establish greater public trust in health IT and facilitate the more rapid adoption of these promising new technologies, privacy and security risks must be addressed. Policymakers and stakeholders should seek to implement a comprehensive framework, while at the same time providing both the detail and the flexibility needed for the complex and evolving e-health environment. In this paper we focused on public policy, but technology design, business practices, and consumer education are also necessary components of the solution. From traditional health entities to new developers of consumer-oriented health IT products to policymakers, all have an important role to play in ensuring a comprehensive privacy and security framework for the e-health environment. The challenge is to find the right mix of statutory direction, regulatory implementation, and industry best practices to build trust in e-health systems and enable the widespread adoption of health IT.

The authors gratefully acknowledge the major support of the Markle Foundation for this work, as well as the support of the California HealthCare Foundation.

NOTES

1. Nearly nine of ten adults (89 percent) want their doctors to electronically exchange information with other doctors, and 71 percent endorse e-prescribing. S.K.H. How et al., "Public Views on U.S. Health System Organization: A Call for New Directions" (New York: Commonwealth Fund, August 2008).
2. Lake Research Partners, American Viewpoint, and Markle Foundation, "Survey Finds Americans Want Electronic Personal Health Information to Improve Own Health Care," November 2006, http://www.markle.org/downloadable_assets/research_doc_120706.pdf (accessed 25 August 2008).
3. See J. Goldman, "Protecting Privacy to Improve Health Care," *Health Affairs* 17, no. 6 (1998): 47–60.
4. Harris Interactive, "Many U.S. Adults Are Satisfied with Use of Their Personal Health Information," Poll no. 27, 26 March 2007, http://www.harrisinteractive.com/harris_poll/printerfriend/index.asp?PID=743 (accessed 15 December 2008).
5. California HealthCare Foundation, "National Consumer Health Privacy Survey 2005," November 2005, http://www.chcf.org/topics/view.cfm?itemID=115694 (accessed 25 August 2008).
6. See the Connecting for Health home page, at http://www.connectingforhealth.org, for a more detailed description of the Common Framework.
7. For a summary of core privacy principles, see the Appendix, online at http://content.healthaffairs.org/cgi/content/full/28/2/416/DC1.
8. Some may qualify as health care clearinghouses to the extent they facilitate the processing of nonstandard data elements into standard data elements. See Section 1171 of the Social Security Act.
9. For a discussion of the problems exchanges have had in building a viable business model, see CHCF, *Privacy, Security, and the Regional Health Information Organization,* June 2007, http://www.chcf.org/documents/chronicdisease/RHIOPrivacySecurity.pdf (accessed 20 November 2008).
10. If a covered entity has a reasonable basis for knowing that the recipient of deidentified data will be able to reidentify those data, the data do not qualify as deidentified. See 45 CFR 164.514(b)(2)(ii).
11. See, for example, S. Ochoa et al., "Reidentification of Individuals in Chicago's Homicide Database: A Technical and Legal Study, November 2008, http://web.mit.edu/sem083/www/assignments/reidentification.html (accessed 15 December 2008).
12. 45 CFR 164.502(b).
13. See U.S. Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information,* pp. 8–10, revised 3 April 2003, http://www.dhhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf (accessed 20 November 2008).
14. HIPAA rules provide for the use of a limited data set—information stripped of certain patient identifiers—for certain purposes. See 45 CFR 164.514(e). Because the difference between deidentified data (via the "safe harbor" method) and the limited data set is only two data categories, HHS may need to develop additional options for use of data stripped of patient identifiers to make this recommendation viable.
15. 45 CFR 164.524(a) and (c) (such access right is for information maintained in a designated record set).
16. DHHS, *Compliance and Enforcement, Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year,* http://www.hhs.gov/ocr/privacy/enforcement/data/top5issues.html (accessed 20 November 2008).
17. State laws may set limits on copying charges for records, which range from free for the first copy (Kentucky) to $37 for up to the first ten pages of a hospital-based record (Texas). See the Georgetown University Center on Medical Record Rights and Privacy home page, at http://hpi.georgetown.edu/privacy/records.html, for more information.
18. See, for example, R.D. Marks, "Regulating Personal Health Records—Why HIPAA Won't Work," 2008, http://www.ehealthinitiative.org/events/papers/Patient_Command_09-01-08.pdf (accessed 20 November 2008).
19. See 18 U.S. Code, sec. 2702 (a)(1)–(3).
20. See ibid., sec. 2701 (c)(1) and sec. 2702 (a)(2)(B).
21. Johns Hopkins University, Genetics and Public Policy Center, Summaries of "Genetic Information Nondiscrimination Act (GINA) Public Law 110-28, Title I: Genetic Nondiscrimination in Health Insurance," http://www.dnapolicy.org/resources/GINATitle1summary.pdf; and "Title II: Genetic Nondiscrimination in Employment," http://www.dnapolicy.org/resources/GINATitleIIsummary.pdf (accessed 15 December 2008).
22. In 2007 the HHS Office of the National Coordinator for Health Information Technology commissioned a

study of thirty policies from PHR vendors and found that none covered all of the typical criteria found in a privacy policy. For example, only two described what would happen to the data if the vendor were sold or went out of business, and only one had a policy with respect to deactivated accounts. See Altarum Institute, *Personal Health Record (PHR) Service Provider Market: Privacy and Security,* 5 January 2007, http://www.hhs.gov/healthit/ahic/materials/01_07/ce/PrivacyReview.pdf (accessed 16 December 2008).

23. According to a 2007 survey, 64 percent of respondents didn't know what a personal health record was, and of those who did, only 11 percent said that they were currently using one. G. Gosselin, "Personal Health Records: More Portable, but Few Seek Access from Health Providers," *Michigan Business Review,* 3 September 2008, http://www.mlive.com/businessreview/tricities/index.ssf/2008/09/personal_health_records_more_p.html (accessed 16 December 2008).
24. See Connecting for Health, "Connecting Consumers: Common Framework for Networked Personal Health Information," 2008, http://www.connectingforhealth.org/phti (accessed 15 December 2008).
25. See S.A. Blevins, "Who's Reading Your Medical Files Today," *Christian Science Monitor,* 26 August 2008; and Deborah Peel, Testimony before the House Subcommittee on Health, Committee on Energy and Commerce, 4 June 2008, http://www.patientprivacyrights.org/site/DocServer/Peel_written_testimony_06.04.08.pdf?docID=4021 (accessed 16 January 2009).
26. See N. Good et al., "Stopping Spyware at the Gate: A User Study of Privacy, Notice, and Spyware," *Symposium on Usable Privacy and Security,* 6–8 July 2005, 43–52, http://cups.cs.cmu.edu/soups/2005/2005proceedings/p43-good.pdf (accessed 16 December 2008).
27. J. Turow, D.K. Mulligan, and C.J. Hoofnagle, "Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace," October 2007, http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf (accessed 25 August 2008).
28. See J. Goldman, Z. Hudson, and R. Smith, *Privacy: Report on Privacy Policies and Practices of Health Web Sites,* January 2000, http://www.chcf.org/topics/view.cfm?itemID=12497 (accessed 2 September 2008).
29. E. Nakashima, "Prescription Data Used to Assess Consumers," *Washington Post,* 4 August 2008.
30. For summaries of state privacy laws, see Health Privacy Project, http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm (accessed 15 December 2008). For federal law, see 42 CFR, Part 2 (2008).
31. Internet technology may make it easier to present short notices, layered notices, and more detailed forms of consent.
32. For example, the National Committee on Vital and Health Statistics has recommended that individuals have the right to decide whether they want to have their identifiable health records accessible through the National Health Information Network. See National Committee on Vital and Health Statistics, *Privacy and Confidentiality in the Nationwide Health Information Network,* 22 June 2006, http://www.ncvhs.hhs.gov/060622lt.htm (accessed 16 December 2008). It also recommended that the NHIN be designed to permit individuals to sequester sections of their health record based on categories of sensitive information. See NCVHS, Letter to the Hon. Michael O. Leavitt, 20 February 2008, http://ncvhs.hhs.gov/080220lt.pdf (accessed 16 December 2008).
33. R. Alonso-Zaldivar, "Effectiveness of Medical Privacy Law Is Questioned," *Los Angeles Times,* 9 April 2008.
34. In July 2008, HHS announced that Providence Health and Services agreed to pay $100,000 as part of a settlement of multiple HIPAA violations, but HHS made clear that this amount was not a civil monetary penalty. See HHS, "HHS, Providence Health and Services Agree on Corrective Plan to Protect Health Information," Press Release, 17 July 2008, http://www.hhs.gov/news/press/2008pres/07/20080717a.html (accessed 15 December 2008).
35. For more information on the Office of Legal Counsel's memo and its consequences, see P. Swire, "Justice Department Opinion Undermines Protection of Medical Privacy," 7 June 2005, http://www.Americanprogress.org/issues/2005/06/b743281.html (accessed 15 December 2008). See also P.A. Winn, "Who Is Subject to Criminal Prosecution under HIPAA?" 2005, http://www.abanet.org/health/01_interest_groups/01_media/WinnABA_2005-11.pdf (accessed 16 January 2009).
36. 45 CFR 164.504(e)(1)(ii).