Rethinking the Role of Consent in Protecting Health Information Privacy

January 2009

This paper advocates for a new generation of privacy protections that allow personal health information to flow among health care entities for treatment, payment, and certain core administrative tasks without first requiring patient consent, as long as there is a comprehensive framework of rules that governs access to and disclosure of health data. Patient consent is one important element of this framework, but relying on consent would do little to protect privacy. This paper also suggests how a framework of protections can provide patients with more meaningful opportunities to make informed choices about sharing their personal health information online.

Slowly but surely, the U.S. health system is undergoing major changes in how patients' health information is collected, stored and shared. Funding and initiatives to establish electronic health information exchange among providers, as well as between patients and providers, are underway. A consensus is emerging that quality health care depends on easy access to reliable and complete patient information. A number of critical policy issues, however, continue to be thorny, not the least of which is how to foster the flow of health information to treat patients and pay for their care, as well as to improve the quality of our health care system and more fully engage patients in their own health care, while at the same safeguarding privacy and security.

Although new innovations in health information sharing hold great promise for more effective and efficient care, they also amplify privacy risks. A system that makes greater volumes of information available more efficiently to improve care will be an attractive target for those who seek personal health information for commercial gain or inappropriate purposes. A significant majority of the public has already expressed concern about the privacy risks associated with health IT, and policymakers will find little public support for building e-health systems if those concerns are not addressed.

It is essential that a policy framework enable the application of information technology for the improvement of health care while allowing people to make meaningful choices about the sharing of their health information. Some advocates have argued that requiring patient consent for every exchange within health care is the solution to the privacy conundrum. However, such an

approach will, in effect, provide fewer privacy safeguards and impose greater burden on individuals, while undermining quality of care and access to services.

What is needed is a new generation of privacy protections that allow personal health information to flow among health care entities for treatment and payment and certain limited administrative tasks without requiring patient consent upfront. Such protections would also allow data to be gathered for important health care quality and public health purposes. However, for most uses outside of this core health care environment, people should be given the opportunity to make meaningful, informed choices about how their identifiable health information is accessed, used and disclosed. Similarly, with respect to giving individuals greater ability to access and store their own health information, these consumer-facing tools and services should similarly provide greater patient control.

This paper begins with a summary of how the current HIPAA Privacy Rule deals with patient consent or authorization. An earlier version of the Rule did require consent for a broad range of uses and disclosures of personal health information, but the final version requires patient authorization for a narrower set of uses and disclosures. While at the time CDT's Health Privacy Project agreed with privacy advocates who vigorously opposed the narrowing of the consent requirement, our thinking has evolved. As explained in more detail below, we now believe that overreliance on consent leads to weak privacy protection. Instead of consent for each and every use, e-health systems should be governed by a comprehensive framework of rules, based on fair information practices, that fill the gaps in existing law, clearly set forth who can access health information and for what purposes, and are vigorously enforced. Patient consent is one component of this comprehensive set of protections, and the second half of the paper suggests in which circumstances patients must be provided with more meaningful opportunities to make informed choices about the sharing of their personal health information on-line.

The Role of Individual Consent or Authorization under the Privacy Rule

The HIPAA Privacy Rule is based on fair information practices and sets forth specific rules governing access, use and disclosure of individually identifiable health information (or protected health information (PHI)) held or transmitted

by "covered entities," which include health plans, health care clearinghouses, and most health care providers who submit health care claims electronically.[1]

In summary, the Privacy Rule permits covered entities to access, use and disclose personal health information without first obtaining a patient's consent for purposes of treatment,[2] payment,[3] and health care operations.[4] The Rule also permits covered entities to access, use and disclose personal health information without patient consent or authorization[5] for certain lawful public health purposes, as required by law, for reporting abuse or domestic violence, for health oversight activities, for judicial and administrative proceedings, and certain law enforcement purposes, as long as proper processes are followed that provide individuals an opportunity to intervene. Covered entities may disclose information to family members, and in health facility or office directories, as long as the patient does not object.

---

1 Specifically, HIPAA applies to any health care provider who transmits health information in electronic form for those transactions for which the Secretary has adopted standards (i.e., transaction code sets). See U.S. Department of Health and Human Services (HHS), Office of Civil Rights Privacy Brief, Summary of the HIPAA Privacy Rule, http://www.hhs.gov/ocr/privacysummary.pdf ("Office of Civil Rights Privacy Brief, Summary of the HIPAA Privacy Rule").

2 Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another. 45 C.F.R. §164.501.

3 Payment includes activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and to furnish or obtain reimbursement for health care delivered to a patient. 45 C.F.R. §164.501.

4 Health care operations include: (1) Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination; (2) Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims; (4) Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; (5) Business Planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and (6) Business management and general administrative activities, including those related implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. 45 C.F.R. §164.501.

5 The HIPAA Privacy Rule uses the term "authorization" when referring to instances where patient consent is required before information can be accessed, used or disclosed. Such authorizations must be in writing and contain specific elements. Throughout this paper, we use the term consent to refer generally to requiring some form of patient permission prior to accessing health information; we use the term authorization when we intend to refer to the particular authorization requirements in the Privacy Rule. See the appendix for a more detailed explanation of how authorization and consent are treated in the Privacy Rule.

The Privacy Rule requires prior patient authorization to use personal health information for marketing purposes (although the definition of marketing includes some exceptions), and for the use of health information for most research (except under certain circumstances). Further, in recognition of the particular sensitivity of certain types of mental health data, the Rule prohibits the disclosure of psychotherapy notes without patient authorization except in certain emergency situations. Importantly, all uses and disclosures of health information that are not addressed by a specific provision in the Privacy Rule require prior patient authorization. Covered entities seeking authorization for a use or disclosure cannot deny treatment or coverage to those patients who decline.[6] In addition, HIPAA expressly does not preempt state health data privacy laws that are more stringent than HIPAA, thus patient consent provisions in state law are preserved. Covered entities are also free to voluntarily adopt consent policies that are more stringent than those in the Privacy Rule. For example, a physician or hospital could decide to obtain patient consent before sharing information for treatment purposes or before sending information to the patient's insurance company.

Finally, covered entities are required to provide individuals with a notice of their rights under the Privacy Rule and how their information may be accessed, used and disclosed for certain purposes without their consent.[7] While such entities must attempt to obtain signatures from individuals acknowledging receipt of the notice, obtaining a signature is not required.[8]

In sum, the overall structure of the HIPAA Privacy Rule allows personal health information to be shared easily for a number of core health care functions - including treatment, payment, public health, quality improvement, and health oversight – as well as to meet certain needs of the legal system. For uses of information outside of those core functions – for example, marketing and other commercial uses of patient information – authorization is required. By adopting this general approach, the Rule meets the needs of the health care system for health data to flow for a wide variety of health-related purposes, while preserving some patient control and requiring authorization for non-health care uses.

Overall, this approach strikes the right balance between the needs of the healthcare system to access information and the rights of patients to exercise some control over this highly sensitive information. As the demands for access to personal health data expand, policymakers must decide which functions are

6 45 C.F.R. §164.508(b)(4).

7 45 C.F.R. §164.520(a) and (b).

8 45 C.F.R. §164.520(c)(2)(II). Only covered health care providers that have a direct relationship with a patient are required to make a good faith effort at written acknowledgement.

core health functions that should be allowed without requiring patient consent and which should require prior patient authorization.

The Health Privacy Project has not always endorsed this approach. As noted above, an earlier version of the Privacy Rule, published on December 28, 2000, required prior patient consent for most routine uses and disclosures of protected health information.[9] However, this version was harshly criticized by members of the health care industry, who argued that the requirements would hinder the delivery of treatment, the processing of payments, and other routine activities by repeatedly requiring consent to be obtained.[10] In response, HHS issued a new version of the Privacy Rule on August 14, 2002, which adopts the current approach.[11]

Some privacy advocates, including several of the authors of this paper, protested the change to the rule because it was perceived as a loss of patient control.

A number of privacy advocates are still calling for reinstatement of the consent-based provisions from the earlier version of the Rule. The position of CDT's Health Privacy Project has evolved. CDT endorses the approach in the current Rule without fully embracing how the approach has been applied, as explained in more detail below. Allowing information to be shared among health care entities without requiring prior consent for a set of core health functions – and requiring authorization for uses and disclosures that are not part of this health care "core" - is good public policy and protects privacy. Requiring consent for each and every use of health information would return information policy to the pre-HIPAA days, when, in the absence of privacy safeguards, providers and payers required patients to sign broad authorizations and then used those authorizations to justify broad information sharing. Those practices created a record of privacy violations that led policymakers to focus on building privacy and security protections into HIPAA. The original provisions requiring prior consent for nearly every use of health information would have provided at best only a perception of privacy, but not meaningful privacy protection.

The section below provides a more detailed explanation of why over-reliance on consent achieves very little in terms of privacy protection – but the two key factors are:

---

9 Standards for Privacy of Individually Identifiable Information; Final Rule, 67 Fed. Reg. 53,182 (August 14, 2002), http://www.hhs.gov/ocr/hipaa/privrulepd.pdf (Final Rule, 67 Fed. Reg. 53,182").

10 HHS, HIPAA Frequently Asked Questions, About the Privacy Rule (November 2006), http://www.hhs.gov/hipaafaq/about/193.html.

11 Final Rule, 67 Fed. Reg. 53,182.

- **Consent under the previous version of the Rule was not meaningful.** Under the prior version of the rule, providers could refuse to treat – and health plans could refuse to cover – any individual who failed to consent to routine uses of their health information. Thus, the power given to patients by requiring consent for treatment, payment, and operations was illusory, because there would have been no meaningful right to refuse.

- **Consent under the previous version of the Rule would have hampered the provision of and payment for health care.** If consent were required for every routine use, providers would be unable to review a patient's record to prepare for a visit, unless the consent covered such a use. Care coordination among providers could be disrupted, as providers would need to seek consent over and over again. Claims payments would be delayed, as providers determined whether the consent covered the information required by the plan for payment, and the plan determined whether their consent covered access to information to pay the particular claim. Because covered entities would be held responsible for accessing or disclosing any information not covered by a patient's consent form, the rule would have either unnecessarily chilled information-sharing even for core health purposes like treatment and payment or resulted in the use of broad blanket consents.

Comprehensive Policy Framework Protects Privacy

Unfortunately, discussions about how to provide privacy protections for electronic health information have been driven by those seeking to reinstate the consent provisions under the earlier version of the Privacy Rule. Focusing on what was "lost" in 2002 pits privacy against information sharing for important, core health care functions – and both are critical to reaping the benefits of health IT. Instead, health and privacy advocates must jointly advance policy solutions that both build public trust and promote the sharing of health information for treatment and improving our health care system. Specifically, health IT must be supported by a comprehensive policy framework that sets clear parameters for access, use and disclosure of personal health information for all entities engaged in e-health and that is vigorously enforced. Patient consent is one important element of this framework – but it should not be the linchpin of privacy protection.

The efficient and effective e-commerce marketplace provides a clear example of why a comprehensive policy framework works better than consent alone to establish trust and facilitate the sharing of personal information. Today, people use credit cards and shop on-line, and many pay bills on-line. However, these

systems work because entities engaged in e-commerce are required to implement secure technologies to transfer financial information and because federal law limits our personal liability if financial information is stolen. The consumer impliedly consents up front by engaging in the transaction (just as a patient impliedly consents up front by seeking care or enrolling in an insurance plan). However, the privacy and security of these transactions is not assured because the individual's consent is sought every time financial information changes hands; it is assured because there is a framework of rules that limits access to data, punishes those who violate the laws, and compensates individuals who suffer financial harm because their information is inappropriately accessed.

A comprehensive policy framework should implement core privacy principles based on fair information practices, but it also should incorporate trusted network design characteristics and establish strong oversight and accountability mechanisms.[12] System design and other technological features offer opportunities to provide stronger protections for personal health information than is possible with paper records. At the network level, electronic health information exchange among providers and health plans can be achieved without creating large, centralized databases that may be more vulnerable to breaches. Strong user authentication and audit trails can control and track access to electronic health information automatically, limiting inappropriate uses and providing a mechanism for detecting those who inappropriately access records. Encryption and other security tools, properly used, erect obstacles to sensitive data access in the event of a breach.

However, such technologies will only be effective if deployed within a strong policy framework. Decisions about technology and standards in the absence of clear policies will de facto establish information policy – and likely will be biased in favor of the interests of data holders. Employing stronger technological safeguards will not build trust in e-health systems if policies permit overly broad access to data. Ideally, security and other technical standards must implement a policy infrastructure that promotes information sharing for core health functions and protects privacy.[13]

The HIPAA Privacy Rule reflects fair information practices. The regulations provide a good starting point for developing the core privacy principles, but they are inadequate even as to traditional health records and are inappropriate

12 See http://www.connectingforhealth.org for a more detailed description of the Common Framework. Other potential sources for policy recommendations include the GAO, the National Committee on Vital and Health Statistics (NCVHS) and the National Governor's Association State Alliance for eHealth.

13 See Carol C. Diamond and Clay Shirky, Health Information Technology: A Few Years Of Magical Thinking? Health Affairs Web Exclusive (August 19, 2008).

to cover the new and rapidly evolving e-health environment. To build consumer trust and ensure that health IT and electronic health information exchange move forward with sufficient protections for privacy and security, policymakers must strengthen HIPAA for records kept by traditional health system participants; fill gaps in HIPAA's coverage where appropriate; establish additional legal protections to reach new actors in the e-health environment; and address the increased migration of personal health information out of the traditional healthcare system.[14]

Why Consent Alone Offers Inadequate Privacy Protection

The ability of individuals to exercise control over their personal health information is one important element of privacy protection, and a comprehensive privacy and security framework should set out circumstances where patient consent or authorization must be obtained. However, consent is not a panacea. As appealing as it may seem in concept, in practice over-reliance on consent puts the burden for data privacy on consumers and provides very weak protection for personal health information in a digital environment.

In isolation, without other legal limits, mandating consent is more likely to lead to overbroad information-sharing than to the protection of patient privacy. Over-reliance on consent can confer disproportionate bargaining power on providers and others seeking approval for disclosure. This is especially true if patients are offered all-or-nothing disclosure options in circumstances in which they are unlikely to withhold consent, or even to understand the choices they are making. In particular, when patients are seeking care or applying for insurance, they often authorize disclosures without a full appreciation of the scope of their consent and with an inadequate understanding of how their privacy is being protected.

Consent obtained at the time of receiving health services or signing up for benefits is particularly suspect. The patient's primary goal at that moment is to get treated. To the patient, the privacy of health information is peripheral to

14 For more information on how HIPAA can be strengthened, see Center for Democracy & Technology (CDT), Comprehensive Privacy and Security: Critical for Health Information Technology (May 2008), http://www.cdt.org/healthprivacy/20080514HPframe.pdf ("CDT, Comprehensive Privacy and Security: Critical for Health Information Technology"); CDT, Statement of Deven McGraw before the House Energy and Commerce Committee on the Discussion Draft of Health Information Technology and Privacy Legislation (June 4, 2008), http://www.cdt.org/testimony/20080604mcgraw.pdf; CDT, Statement of Deven McGraw before the Subcommittee on Health, Committee on Ways & Means on Promoting the Adoption and Use of Health Information Technology (July 24, 2008), http://cdt.org/testimony/20080724mcgraw.pdf ("CDT, Ways & Means Testimony").

that transaction. Patients are not focused on the ways their information might be used in the future. It is questionable whether a patient is making an informed choice in consenting to disclosure at that time.[15]

The limits of consent were illustrated recently by reports of health and life insurers obtaining personally identifiable prescription drug information from commercial data miners.[16] The revelation was greeted with expressions of concern, but the transactions were in fact based on consent: individuals had consented to the release of their data as a condition of insurance, and the data miners had obtained the drug records legally pursuant to that consent.

Simply stated, consent is not the sine qua non of privacy protection. Equating privacy with consumer consent relieves the holders of patient data of the responsibility for adopting comprehensive privacy protections. If the health care industry were directed simply to solve privacy concerns with consent, it would have less incentive to design and implement systems with technological and operational protections for privacy. In other words, if industry can rely on a consent form to authorize all potential uses and disclosures of personal health information, there is little reason to design networks to minimize risks to privacy, spend scarce resources on ensuring that systems incorporate the latest security technologies (such as encryption or role-based access controls), or train staff in the permitted uses and disclosures of health information. Further, the role of enforcement would be reduced to a mere check on whether the use or disclosure was covered by the consent form instead of ensuring that data holders are following clear rules regarding how health information can be used and disclosed.

The problem is exacerbated by consent forms and privacy notices that are written in language the average person cannot understand. A "consent for every use" approach means privacy will depend on an individual's ability to read and fully understand a consent form and the potential uses of their health information covered therein. Rarely do individuals focus on the details of consent forms, and many do not understand them. Further, many patients wrongly assume that the existence of a "privacy policy" means that their

---

15 Priscilla Regan, The Role of Consent in Information Privacy Protection, in Considering Consumer Privacy: A Resource for Policy Makers and Practitioners, edited by Paula Bruening, pg. 25 (2003), http://www.cdt.org/privacy/ccp/consentchoice2.shtml/pdf.

16 Chad Terhune, They Know What's In Your Medicine Cabinet, Business Week, July 23, 2008, http://www.pnhp.org/news/2008/july/they_know_whats_in_.php; see also Ellen Nakashima, Prescription Data Used To Assess Consumers, Washington Post, August 4, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/08/03/AR2008080302077.html.

personal information will not be shared, even when the policy and the accompanying consent form say just the opposite.[17]

Even when forms are written in simpler language, too often they are drafted to persuade patients that compromising their privacy is to their advantage.[18] The sheer volume of forms that can confront a patient is also a factor. Patients can face "consent fatigue" upon encountering too many consent forms, and information overload makes it less likely that patients will even try to understand the terms of disclosure.[19] Presented with frustratingly complex paperwork, patients are less likely to expend the effort necessary to understand the terms of each form.[20]

Strengthening the Role of Consent

However, just because consent alone is an inadequate safeguard does not mean it has no role in protecting privacy. Patient consent should be viewed as one element of a comprehensive framework of privacy protections for personal health information, and any requirements for patient consent or authorization

---

17 Nathaniel Good, Rachna Dhamija, Jens Glokklags, David Thaw, Steven Aronowitz, Deirdre Mulligan, and Joseph Konstan, Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware, http://www.icsi.berkeley.edu/pubs/bcis/Spyware.pdf; see also Joseph Turow, Deidre K. Mulligan, and Chris Jay Hoofnagle, Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace, University of Pennsylvania Annenberg School for Communications and UC Berkeley Law's Samuelson Law, Technology & Public Policy Clinic (October 2007), http://www.law.berkeley.edu/clinics/samuelson/annenberg_samuelson_advertising-11.pdf.

18 For example, a popular insurance company in the Washington, D.C. area recently sent forms to its enrollees seeking their consent to participate in a completing a "free, confidential survey," that would result in the generation of a "confidential personal health profile" that could be viewed anytime by the individual and reviewed with a physician. At the very end of the letter was the following:

All personal health information exchanged between you and [name of health profile company] will be kept confidential. The information will only be shared with your group health plan and/or your employer for purposes of administering the group health plan.18

The letter tries to assure plan enrollees that their information will be kept confidential; but it also authorizes the use of the personal health information provided by the enrollee in completing the health profile for a potentially broad range of "administrative" activities. The average consumer, who doesn't have a sophisticated understanding of the health care system, is unlikely to grasp the breadth of uses that could be made of information voluntarily provided by the consumer who is seeking to obtain the benefits of completing this profile. (Letter on File with CDT).

19 Marie Pollio, The Inadequacy of HIPAA's Privacy Rule: The Plain Language Notice of Privacy Practices and Patient Understanding, 60 N.Y.U. Ann. Surv. Am. L. 579 (2005), http://www1.law.nyu.edu/pubs/annualsurvey/documents/60%20N.Y.U.%20Ann.%20Surv.%20Am.%20L.%20579%20(2005).pdf.

20Amichai-Hamburger et al., The Effects of Learned Helplessness on the Processing of a Persuasive Message, 22 Current Psychology 1: 37- 46 (2003).

should be an adjunct to clear rules that limit how the information can be accessed, used and disclosed and that are adequately enforced. There is much that policymakers should do to strengthen the role of patient consent. Below we discuss how the Privacy Rule can retain its general approach - allowing core health functions to take place without requiring consent - and yet still enhance the role of individual control in its framework of protections. For example, we recommend:

- Tightening the definition of "marketing" in the HIPAA rule to strengthen a patient's right not to have personal health information used for marketing purposes without consent;
- Narrowing the category of health care operations;
- Expanding consent with respect to having information accessible through health information exchanges; and
- Strengthening the role of consent in personal health records.

Each is discussed in more detail below.

Policymakers should also consider setting standards or issuing guidance or best practices for consent, in order to respond to the limits and weaknesses of consent described in this paper. For example, consent should ideally be part of a process of patient education, not just a form to sign or a box to check.[21] Dialogue between provider and patient can enhance understanding of what is at stake in giving or withholding consent.[22] Consent forms and privacy notices also should be simplified and more readable.

The recent and substantial growth of health IT presents an unprecedented opportunity to integrate consent more fully into the patient experience, provide individuals with meaningful consent management mechanisms, and move beyond blanket consents that have deprived patients of the more nuanced choices necessary to protecting the privacy of health information in the digital era. The same technological creativity and innovation that have spurred the development of electronic health information can and should be applied to the creation of next-generation consent mechanisms and privacy controls. A critical and complementary task to that of crafting appropriate policy responses is identifying how to best leverage technology to put individuals in control of their health information.

Tightening the Definition of Marketing under HIPAA

---

21 American Medical Association, Informed Consent, http://www.ama-assn.org/ama/pub/category/4608.html.

22 Sunil Kripalani et al., Clinical Research in Low-Literacy Populations: Using Teach-Back to Assess Comprehension of Informed Consent and Privacy Information, IRB: Ethics & Human Research; Mar/Apr 2008, Vol. 30 Issue 2, p.13-19.

Although HIPAA already prohibits use of health information for marketing without patient authorization, the definition of marketing includes significant exceptions.[23] These exceptions permit the use of a patient's personal information without consent to facilitate communications from health care providers and plans that can be characterized as patient education (for example, information on treatment alternatives, or benefit options, or care management tools). As a result, there are few communications sent by HIPAA covered entities that are not covered by one of the exceptions. In fact, the only health-related communications that are clearly marketing – and prohibited without express patient authorization – are those made directly by a third party selling a product or service, where the covered entity has provided the third party with the personal information that facilitates the making of the communication.[24] However, if the communication about that same product or service is sent by the covered entity to the patient, it is not marketing – even if the covered entity is paid by the third party to make the communication on its behalf.

Tightening the rules regarding use of personal health information for marketing purposes would greatly enhance patient trust. A 2006 Markle Foundation study examining individuals' views about having their health information on-line showed three-fourths of consumers were concerned that their health information would be used for marketing purposes.[25]

Policymakers should close the regulatory loophole that allows outside entities to have their products and services marketed to patients without their consent. Policymakers could also narrow the definition of marketing or more precisely describe the types of communications that may be sent without authorization. For example, the Rule could permit the use of personal information to send reminders to patients about refilling current prescriptions or getting an annual flu shot in lieu of a more broadly worded health exception that is easily exploited. For communications that policymakers want to exempt from authorization because they are arguably beneficial to a patient's health, policymakers also could limit the types of personal information that can be used for this purpose to merely demographic information (not actual health information), or they could at least allow patients to opt-out of these educational communications. All of these options would give patients greater power over having their information used to generate unwanted solicitations.

Narrowing the Category of Health Care Operations

---

23 45 C.F.R. §164.501.

24 Office of Civil Rights Brief, Summary of the HIPAA Privacy Rule, p. 9-10.

25 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.

Under the current Privacy Rule, patient consent is not required for covered entities to use personal health information for health care operations. The definitions of treatment and payment are relatively narrow; however, health care operations encompasses a much wider range of activities, including certain administrative, financial, legal, and quality improvement activities.[26] Privacy and consumer advocates have long been concerned that health care operations permits the use of personal health information for a broader range of purposes than should be permitted under fair information practices.

Some have proposed requiring patient consent for health care operations as a way to limit the use of patients' identifiable information for purposes beyond what is fair and appropriate. However, consistent with the information-sharing approach outlined in this paper, patient consent should not be required for those activities within "health care operations" that are necessary to support the core health care functions of treatment and payment. Requiring consent for these core health care operations is not the correct approach, for two key reasons. First, providers and payers would likely condition treatment or payment on use of information for these purposes, because they are core to treatment and payment. Second, covered entities might use consent to circumvent current rules that are designed to minimize the amount of data accessed or disclosed for a particular purpose. A broadly worded consent for use of information for operations purposes could result in broader access to or disclosure of data than occurs today under the "minimum necessary" standard in the Rule.

HHS should re-examine the health care operations definition with a framework approach in mind, allowing uses without consent for a core set of health care operations, subject to the minimum necessary standard, and requiring patient authorization for those that may be desirable but are not necessary to facilitate core treatment and payment functions. HHS should also consider crafting more narrow definitions of, or providing more detailed guidance regarding, some of the broad terms used in health care operations (such as "case management and care coordination") to ensure they are defined to include only core functions.

Further, HHS should consider whether fully identifiable patient data is needed to accomplish all of the activities currently included in health care operations, and whether data scrubbed of common patient identifiers, which provides greater privacy protection for patients, could serve covered entities' needs to access data without being unduly burdensome. For example, today covered entities may use fully identifiable data for quality assessment and improvement activities, peer review of health professionals, accreditation or credentialing, performing audits, and business planning. For each of these activities, covered

26 See footnote 4 for the definition of health care operations.

entities need access to data about the care that was provided, but in most cases they do not need information that is identified to a particular patient. Using data that has been stripped of key patient identifiers can help protect privacy while allowing the use of data for important health-related functions. The Privacy Rule includes provisions for two types of anonymized data – the limited data set and de-identified data. However, these data sets likely require the masking of too much data to be useful for many operations purposes. HHS should examine additional options for use of data stripped of common patient identifiers for operations purposes.

Expanding Consent with Respect to Data Accessible Through Health Information Exchanges

The vehicles for electronic health care information exchange provide additional opportunities to strengthen the role of consumer consent in e-health. State and regional electronic health information exchanges – often called Regional Health Information Organizations (or RHIOs) or Health Information Exchanges (HIEs) – typically facilitate the electronic exchange of personal health information among providers and often between providers and plans. The models for these exchange entities are still in development, but HHS' overall plan (begun during the Bush Administration) is that these entities will be linked up to form the National Health Information Network (NHIN), which will provide a secure, nationwide, interoperable health information infrastructure connecting providers, consumers, and others involved in supporting health and healthcare.[27]

But while RHIOs and HIEs may change the health care landscape by improving care and decreasing costs, issues related to privacy and security present substantial challenges and even barriers for these exchanges. It is imperative that adequate policies and standards are in place to protect the privacy of patients whose information is held in, managed by, or exchanged through a health information exchange. In setting appropriate privacy and security policies and standards for health information exchanges, policymakers must consider the degrees of risk posed by the different exchange models. The architecture of a particular exchange raises different privacy and security risks, which require tailored policy responses to appropriately address them. For example, the Markle Foundation's Common Framework Resources for Implementing Private and Secure Health Information Exchange, released in 2006, sets forth different types of policies networks can adopt to protect patient privacy and security. For exchange among providers and plans, the Common Framework recommends a "network of networks" approach that helps ensure

27 HHS, Centers for Medicare & Medicaid Services, Are you a Covered Entity?, http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp.

the privacy and security of information being exchanged.[28] Specifically, the health information remains stored with the providers and institutions that have the direct relationships with patients. Those entities make decisions, consistent with applicable law, regarding policies for health information sharing - i.e., they retain legal responsibility for the personal health information they maintain and make local determinations about what information will be shared through the network.

At a minimum, health information exchanges should be required to comply with HIPAA privacy and security regulations, either as covered entities or business associates depending on their structure and functions. For example, exchanges that merely facilitate the exchange of data among covered entities should 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 should be covered entities. (This is a similar approach to how the Privacy Rule treats healthcare clearinghouses.) Recently, HHS issued guidance stating that exchanges that transmit data among covered entities must be business associates of those entities.[29] Although this guidance is welcome and long overdue, it does not address those exchanges that store data or that have independent rights to access or disclose data.

However, ensuring that these exchanges are subject to HIPAA rules is not sufficient. Health information exchanges are still a nascent sector and their business model is in flux.[30] Although these new exchanges typically begin by collecting patient data only for treatment purposes, many are learning that it is difficult to generate sufficient operating income through data exchange, and also some are looking at tertiary uses of data to generate income. Because such uses may one day become the industry norm, and because of the "game-changing" nature of these networks, it is prudent to also require patient authorization as a safeguard early in their development. Patients should be given a choice for uses or exchanges of their information for purposes other than their treatment. Exchanges that do not provide patients with a meaningful choice should be limited to sharing information for treatment purposes only.

The Privacy Rule provides patients with a right to request a restriction on the uses and disclosures of their PHI for treatment, payment or health care

---

28 Markle Foundation, Connecting for Health, http://www.connectingforhealth.org.

29 HHS, Office of Civil Rights, The HIPAA Privacy Rule and Health Information Technology, http://www.hhs.gov/ocr/hipaa/hit/.

30 New York Statewide Collaboration Process (SCP) and New York Health Information Security and Privacy Collaboration (HISPC), Recommendations for Standardized Consumer Consent Policies and Procedures for RHIOs in New York to Advance Interoperable Health Information Exchange to Improve Care (September 2008)(copy on file with CDT)("SCP and HISPC, Recommendations for Standardized Consumer Consent Policies and Procedures for RHIOs in New York").

operations, disclosure to persons involved in a patient's health care or payment for care, or disclosure to notify family members or others about the patient's general condition, location, or death.[31] However, covered entities are under no obligation to honor such requests.[32] If a covered entity does agree to the request, it must comply with agreed-upon restrictions, except for purposes of treating the patient in a medical emergency.[33] Thus, if exchanges were subject to the Privacy Rule, they would not be required to provide patients with a right to consent to having their data included in the exchange or to honor any requests to restrict access to data via an exchange.

Without a meaningful right to restrict data, individuals with heightened concerns about having their personal health information accessible through a regional or statewide exchange, or the National Health Information Network, are left without any recourse. They may be more likely to engage in "privacy protective" behaviors, including paying out-of-pocket for services, visiting physicians out of the network, or steering clear of care altogether, to avoid the risks associated with having their personal health information more easily accessed through a health information exchange.

A number of experts are recommending that patients have some right to control whether or not their information is included in an electronic exchange – and a number of exchanges are implementing policies and practices that support some level of patient consent. The Markle Common Framework for Health Information Exchange recommends giving patients control by allowing them to create a second or third identity for records they want to keep out of the networked electronic records exchange.[34] In 2006, the National Committee on Vital and Health Statistics (NCVHS) recommended that HHS assess the "desirability and feasibility of allowing individuals to control access to the specific content of their health records via the NHIN, and, if so, by what appropriate means."[35] NCVHS followed up early in 2008 recommending that individuals have the right to keep certain sensitive categories of health information out of a health information exchange.[36] Under NCVHS' proposed

---

31 45 C.F.R. §164.522(a)(1)(B).

32 45 C.F.R. §164.522(a)(1)(B)(ii).

33 45 C.F.R. §164.522(a)(1)(B)(iii). In addition, a restriction agreed to by a covered entity is not effective under this subpart to prevent uses or disclosures permitted or required under §164.502(a)(2)(ii), §164.510(a), or §164.512. 45 C.F.R. §164.522(a)(1)(B)(v).

34 Markle Foundation, Connecting for Health, http://www.connectingforhealth.org/.

35 National Committee on Vital and Health Statistics (NCVHS), Letter to the Secretary, Recommendations regarding Privacy and Confidentiality in the Nationwide Health Information Network, (June 22, 2006), http://www.ncvhs.hhs.gov/060622lt.htm.

36 NCVHS, Individual control of sensitive health information accessible via the Nationwide Health Information Network for purposes of treatment (February 20, 2008), http://ncvhs.hhs.gov/080220lt.pdf.

approach, healthcare providers accessing an individual's record through an exchange would not see any information in the restricted category, though individuals would have the further option of consenting to a specific provider's access to the sequestered information.[37] Providers would see a notation in the record indicating that information was blocked; NCVHS left for further discussion whether the notation should be general or should indicate the category of information blocked.[38] NCVHS acknowledged that implementing the recommendation would be challenging but argued that offering patients this level of individual control was worth the undertaking.[39]

Current consent practices of exchanges across the country vary. For example, as of mid-2008, the Regenstrief-administered Indiana Network for Patient Care (INPC)[40] does not require patient consent for participation in the exchange. Rather, patients who wish to opt out must approach their provider for a HIPAA request for restriction, which pursuant to the Privacy Rule does not have to be granted. However, physicians are not required to include a patient's record in the exchange; thus, a provider may honor a patient request that her records not be accessible through the network by not uploading or making them available to the exchange at the outset.[41] One type of record is categorically excluded; INPC does not collect or transmit psychotherapy notes.[42] Nevada and Wisconsin also do not require patient consent to exchange health information for treatment purposes.[43]

The Tennessee-based MidSouth Health Alliance[44] also does not require patient consent for its data exchange. Instead, MidSouth provides patients with a notification form and allows them to opt-out of the exchange at the hospital or clinic level.[45] MidSouth also has an exception to its general rule, as it operates a DNA databank on an opt-in basis.

Other examples of consent practices include New York, where a patient must consent to the exchange of health information in the statewide exchange SHIN-

37 Id.

38 Id at 5-6.

39 Id at 10.

40 Regenstrief Institute, Indiana Network for Patient Care, http://www.regenstrief.org/medinformatics/inpc.

41 Id.

42 Id.

43 Kristin Rosati, Arizona Health-e Connection, Summary of Other HIE Approaches (September 2008)(copy on file with CDT).

44 MidSouth Health Alliance, http://www.midsoutheha.org.

45 Id.

NY for non-emergency treatment.[46] Rhode Island requires consent for release of health information to the state exchange and for provider access to health information in the exchange, with some exceptions.[47]

In the absence of a national policy regarding consent, multistate collaborations are working to craft solutions. The Health Information Security and Privacy Collaborative (HISPC), established by RTI International in June 2006 under a contract from HHS, was formed to address the privacy and security challenges presented by electronic health information exchange.[48] In April 2008 HISPC began its third phase, and now includes 42 states and territories.[49] This latest phase is focusing on: 1) analyzing consent data elements in state law; 2) studying intrastate and interstate consent policies; 3) developing tools to help harmonize state privacy laws; 4) developing tools and strategies to educate and engage consumers; 5) recommending basic security policy requirements; and 6) developing inter-organizational agreements.[50] The results of this work could help inform policymakers at the local, state and national levels.

It may be premature to mandate a particular patient consent model at the federal level that would apply to all exchanges. However, policymakers have an important role to play in the development of privacy and security standards to govern health information exchanges. Exchanges may offer improvements to an increasingly fragmented and costly health care system, but the risks of such exchange are palpable. In addition to ensuring that there is a strong framework of rules governing the activities of these exchanges, there are specific steps policymakers can take to expand consent with respect to health information exchange. For example, they can require local exchanges to develop policies on

---

46 New York Public Health Law, Section 18, requires consent for use of information for all purposes except in an emergency; thus, New York officials concluded that its information exchanges would be opt-in. See SCP and HISPC, Recommendations for Standardized Consumer Consent Policies and Procedures for RHIOs in New York.

47 Rhode Island Health Information Exchange, http://www.riqi.org/matriarch/MultiPiecePage.asp_Q_PageID_E_25_A_PageName_E_StrategicInitTTCHealthInfoExch.

48 Health Information Security & Privacy Collaboration, http://privacysecurity.rti.org/; see also http://privacysecurity.rti.org/Portals/0/HISPC_Exec_Summary_2008.pdf.

49 During Phase 1, the 34 participating states and territories (1) assessed variations in organization-level business policies and state laws that affect health information exchange; (2) identified and proposed practical solutions, while preserving the privacy and security requirements in applicable federal and state laws; and (3) developed detailed plans to implement solutions. In Phase 2, each of the 34 participants selected a foundational component of their larger implementation plan to be completed in a 6-month time frame. During this phase, additional states and territories were encouraged to participate in HISPC's third phase, which includes seven multistate collaborative privacy and security projects, and which began in April 2008. Id.

50 Id.

patient consent, and ensure that patient and consumer organizations have meaningful roles in developing these policies. Further, employment, insurance coverage, or treatment should not be conditioned on patient participation in an electronic exchange network.

Strengthening the Role of Consent in Personal Health Records

Personal health records (PHRs), which give consumers a mechanism for storing and sharing their own (or a family member's) health information, provide unique opportunities to get consumers more engaged in their own health care. The information in a PHR may be a copy of a record downloaded or sent by a provider or plan, or the patient may enter it. There is no single common definition or model of a PHR.[51] A variety of types are being offered to consumers today – ranging from Internet-based health information platforms being offered by Google, Microsoft, and Dossia; to PHRs offered by Kaiser Permanente and other payers and providers; to health record banks, which are independent organizations that furnish a secure electronic repository for storing and maintaining a patient's medical and other health records.[52]

The HIPAA Privacy Rule covers PHRs offered by entities covered by HIPAA.[53] Internet-based PHRs supplied by Google, Microsoft, and Dossia are not covered by the Rule, which means that the information in the PHR is not protected by any federal health information privacy law.[54] CDT has argued against application of the HIPAA Privacy Rule to consumer-based health information tools and services. Instead, the Federal Trade Commission (FTC) and HHS

---

51 NCVHS, Personal Health Records and Personal Health Record Systems (February 2006), http://ncvhs.hhs.gov/0602nhiirpt.pdf.

52 William A. Yasnoff, Electronic Records are Key to Health-Care Reform, Business Week, http://www.businessweek.com/bwdaily/dnflash/content/dec2008/db20081218_385824.htm.

53 HHS, Office of Civil Rights, Personal Health Records and The HIPAA Health Privacy Rule, http://www.hhs.gov/ocr/hipaa/hit/PHR.pdf.

54 A variety of federal and state laws may apply to companies that offer PHRs to consumers, including federal and state consumer protection laws enforced by the Federal Trade Commission and state consumer protection agencies, and state contract and negligence (tort) law enforced through litigation. Broadly speaking, these laws require companies offering PHRs to be fair in how they advertise features of their PHRs and in how they explain the rules of use, limitations, and risks of their PHR systems. See http://www.healthprivacy.org/. Some PHRs also may be subject to the provisions of the Electronic Communications Privacy Act and Stored Communications Act, which primarily regulate government access to electronic communications and records. None of these laws is sufficient to provide comprehensive protections for consumers using PHRs, a conclusion CDT will explain in more detail in a separate paper on PHRs that will be published in early 2009.

should develop privacy and security requirements for PHRs that target the unique privacy risks faced by consumers using PHRs.[55]

But, regardless of whether a PHR is covered by the Privacy Rule, the most common PHR models today are giving consumers sole or a high degree of control over the personal health information contained in the PHR account.[56] Since the purpose of PHRs is to give consumers tools they can use to maintain and improve their health (and the health of their family members), it is critical that PHRs continue to offer consumers the highest possible degree of control over their information – and public policies should reinforce this trend. In 2008 the Markle Foundation's Connecting for Health initiative released a new Common Framework specifically for consumer-facing technologies like PHRs. The "Common Framework for Networked Personal Health Information" recommends that no information in the PHR be accessed or disclosed without the consumer's consent. The Common Framework also includes recommendations to make such consent more meaningful (for example, by recommending that it be readable as well as amendable, revocable and contextual).[57] CDT's Health Privacy Project also worked with a group of employers to develop Best Practices for Employers Offering PHRs.[58] These "best practices," released in 2007, also include giving individuals (employees) control over who has access to information in their PHR.[59]

NCVHS also has recommended that consumers have the right to make an informed choice concerning the uses of their personal information when signing up to use any personal health record products or services.[60] Further, the Confidentiality, Privacy and Security Workgroup of the American Health Information Community (AHIC) recently recommended that uses and disclosures of personal health information in PHRs be subject to consumer consent,[61] and the eHealth Initiative's Blueprint: Building Consensus for

---

55 CDT, Comprehensive Privacy and Security: Critical for Health Information Technology; see also CDT, Ways & Means Testimony.

56 See http://www.google.com/intl/en-US/health/about/privacy.html; http://account.healthvault.com/help.aspx?topicid=PrivacyPolicy; http://www.dossia.org/consumers/privacy-statement.

57 Markle Foundation, Connecting for Health, Common Framework for Networked Personal Health Information, http://www.connectingforhealth.org/phti/.

58 See http://www.cdt.org/healthprivacy/ for more information on this initiative.

59 The Employers' Working Group on PHRs, which was convened by the California Healthcare Foundation and IBM and staffed by the Health Privacy Project, included Dell, Google, Hewitt Associates, the Markle Foundation, Omnimedix Institute, Pfizer, Pitney Bowes, Revolution Health, Wal-Mart, and WebMD.

60 NCVHS, Personal Health Records and Personal Health Record Systems (February 2006), http://ncvhs.hhs.gov/0602nhiirpt.pdf.

61 Letter from CPS Workgroup to HHS Secretary Leavitt (September 23, 2008),

Common Action also included provisions recommending consumer control for information in PHRs.[62]

Notwithstanding the strong role for consent in these consumer-facing health IT models, CDT does not recommend relying on consent as the sole mechanism for protecting the privacy of personal health information stored in or shared through these tools, for all of the reasons discussed in this paper. The Markle Common Framework for Networked Personal Health Information also sets forth a set of privacy principles for PHR providers, whether or not they are covered by HIPAA.[63] CDT has endorsed these principles, as have major PHR vendors and a number of consumer organizations.[64] The Certification Commission for Health IT (CCHIT), which is seeking to certify PHR systems for their privacy and security features, is relying on this Common Framework in developing its certification criteria.[65] The Employer Best Practices for PHRs referenced earlier could also be used by policymakers to craft appropriate legal protections. CDT's specific recommendations for legal protections for personal health information in PHRs will be dealt with in more detail in a separate paper to be published in early 2009.

Conclusion

Patients' ability to exercise control over their health care information is an integral part of health information privacy, particularly as the health care system undergoes change in how health information is collected, stored, and shared. However, consent should not be the anchor for protecting privacy. Requiring consent for every exchange within health care would provide fewer privacy safeguards and impose a greater burden on patients, while undermining quality of care and access to health care services.

CDT advocates a new generation of privacy protections that allow personal health information to easily flow for treatment, payment, and certain core administrative tasks without requiring patient consent, with more meaningful

---

http://www.hhs.gov/healthit/documents/m20080923/06b_cps_letter.html.

62 eHealth Initiative Blueprint, Phase 1 (October 10, 2007), http://www.ehealthinitiative.org/blueprint/eHiBlueprint-BuildingConsensusForCommonAction.pdf.

63 Markle Foundation, Connecting for Health, CP3: Consumer Consent to Collections, Uses, and Disclosures of Information, http://www.connectingforhealth.org/phti/reports/cp3.html.

64 Endorsers include AARP, America's Health Insurance Plans, Dossia, Google, Intuit, Microsoft, the National Partnership for Women & Families, and WebMD.

65 Certification Commission for Health Information Technology Personal Health Records Work Group, Introduction to First Draft 09 Criteria (September 29, 2008), http://www.cchit.org/files/comment/09/01/CCHITCriteriaPHR09Intro.pdf.

consent required in certain key contexts. There must be a comprehensive framework of rules, based on fair information practices, that fill the gaps in existing law and clearly set forth who can access health information and for what purposes, and that are vigorously enforced. Innovative technologies that create a more robust consent experience and give individuals more nuanced control over their health information should serve to support and complement these rules. Within this framework, there are ways to strengthen the role of consent, particularly with respect to the new e-health technologies, while still allowing for the flow of information in core health exchanges. Technology can help enhance patient control of information and ensure that, when consent is sought, it is honored as information moves throughout the health care system.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION

Please contact: Deven McGraw, (202) 637-9800 x 119, deven@cdt.org

APPENDIX: Authorization and Consent

Conceptually, consent and authorization accomplish the same goal: ensuring that an individual agrees to particular uses and disclosures of their health information. But the Privacy Rule treats consent and authorization differently. Specifically, consent is not required for disclosures for treatment, payment or health care operations (TPO), but covered entities may require such consent voluntarily (or in accordance with applicable state law). Authorization is required for all disclosures that are not TPO and that are not expressly authorized by a specific provision in the Rule (e.g., disclosures for law enforcement and public health purposes). When authorization is required, it must be in writing and include specific elements. In most cases, treatment or payment may not be withheld if a patient declines to authorize the particular use or disclosure.

Consent is not defined in the Rule, but guidance from HHS defines it as written permission from individuals to use and disclose their health information.[66] The content of a consent form or the process by which the entity obtains consent is not described in the Privacy Rule.[67]

An authorization is required to give covered entities or third parties permission for certain uses and disclosures of health information, most notably for marketing and use of psychotherapy notes.[68] Covered entities generally may not condition an individual's treatment or coverage on providing authorization.[69] The requirements of a valid authorization are more stringent than a voluntary consent.[70] Authorization must specify certain details, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed."[71] Authorization forms must be written in "plain language."[72]

66 Office of Civil Rights Privacy Brief, Summary of the Privacy Rule, p. 5.

67 Id.

68 HHS, HIPAA Frequently Asked Questions, Authorization Use & Disclosure, http://www.hhs.gov/hipaafaq/use/264.html.

69 Id.

70 45 CFR §164.508(c).

71 Id.

72 45 C.F.R. §164.508(c)(3).