Whose Data Is It Anyway?

Expanding Consumer Control over Personal Health Information

California HealthCare Foundation

ISSUE BRIEF

February 2008

Introduction

Health information in the United States is largely possessed and controlled by clinicians who provide care and by insurance companies and other entities who pay for care. While federal and state laws give consumers the right to obtain paper copies of their medical records, the terms of such transactions may be onerous. Moreover, the information cannot be readily transmitted and, for both patients and providers of care, generally is not useful in care delivery, outcomes analysis, or biosurveillance.

California's law is typical. Within 15 days of a patient's request, the clinician must provide a paper copy of that individual's records at a cost of 25 cents per page.[1] For many patients, especially the chronically ill, who have voluminous records and see multiple clinicians, access to personal health information under these terms is too expensive and involves unacceptable delays in gaining access to vital data.

As health care transitions from paper-based to electronic records, there is a significant opportunity to expand the traditional concept of consumers' rights to access and use their personal health information. Indeed, such access and use are crucial prerequisites to realizing the full potential of technologically driven advances in the health care system.

This policy brief explores important issues that must be addressed if consumers are to have meaningful legal rights to access, use, and control their electronic health information through a personal health information custodian serving on their behalf.

Key Findings

- Redefining consumers' rights will require a fundamental shift from the current legal structure, in which clinicians control medical records and determine the permissible circumstances for disclosing the information in them, to a new legal structure in which consumers have an affirmative right to access electronic information regardless of its source and to use it as they deem necessary.
- New laws could give consumers the right to direct that a copy of any personal health information stored in a standardized electronic format be sent to the custodian of their choice, and ensure that the custodian uses the information in a manner specified by the consumer.
- Current regulation of personal health information under federal and state law is fragmented. Because federal law does not preempt more stringent state privacy laws, and because Congress has not chosen to act, states may have to take the near term reform initiative.
- New laws will require a clear definition of "personal health information custodian." They should also include safeguards under consumer protection laws to ensure that such information remains secure and is not used inappropriately, affirm the right of consumers to send and store the information as they see fit, and set fees for electronic transmissions of medical data from providers to patients.
- Economic incentives for clinicians to adopt a technology enabling them to convey personal

health information to patients would facilitate the transition to a new legal framework. Eventually, this capability might be required as a condition for receiving federal reimbursement under Medicaid, Medicare, or other government-financed programs.

Background

Mounting evidence indicates the importance of engaging patients directly in their care.[2] Yet in today's health care environment, consumers typically must gather and store personal health information on paper. Collecting such information from multiple providers is time-consuming and burdensome. The information often is fragmented and incomplete, and transmitting it to other providers is onerous for consumers and providers alike.

Perhaps most importantly, the information is in a format that is meaningless to patients and, if scattered among different locations, may not be accessible to caregivers. This leaves even the most educated and committed patients without a crucial tool for taking an active role in their care.

A New Health Information Paradigm

Consumers now expect to be able to access various types of information on the Internet. With rising adoption of health information technology and the increasing ability to collect, store, and exchange information electronically, a growing number of consumers also expect to be able to access their personal health data.

In an ideal, electronically enabled health care system, consumers could:

- Easily transmit discrete portions or comprehensive files of their data to the caregiver(s) of their choice for direct care or other purposes, on demand and in a matter of seconds.
- Access a copy of their personal information from various sources, store the information in one location, and automatically receive updates—including notification of changes—from these sources.
- Organize the information in formats that are meaningful to them and their health care providers, and take advantage of features that educate them and help them participate in their care.
- Search through their personal health information more easily and efficiently—for example, to find the name of a particular drug or to access an old care plan for a long-term chronic condition.

Personal Health Information Custodians

The potential role of personal health information custodians, or third parties, in helping consumers obtain, organize, and use their information to improve their health is gaining recognition. Internet and technology companies, federal and state policymakers, employers, insurers, and foundations are exploring the technical infrastructure that could support a custodial system, the policies that would govern it, its financial feasibility, and the potential clinical benefits to patients and society.[3]

As these players know, health care in the future will be powered by rapid technological advances that bring new opportunities to engage consumers in personalized disease management and other activities aimed at improving the quality and efficiency of care. However, this new paradigm will also pose greater risks, such as security breaches and the inappropriate use or sale of personal health information by commercial interests. To fully realize potential quality and efficiency gains, consumers will need greater access to their personal health information, and assurances that the information is protected from such risks.

An increasingly antiquated legal structure is significantly shaping the technological, operational, and business models that are evolving for the custodianship of personal health information. The creators of this structure did not fully anticipate the change from paper-based to

digital health records nor contemplate the possibilities of consumer-centered health information exchange.

Custodial Models

A variety of health information custodial models are evolving. They include:

- **Provider-based personal health records.** Via a Web portal, consumers can call up personal health records (PHRs) kept by a health care provider to view their personal health information in an emergency, schedule appointments, send email to or receive email from a physician, consult with a health care professional, take advantage of educational programs that help them better understand and self-manage medical conditions and medications, or perform other tasks.

  Under this model, health information generally is tethered to the clinician who is its source, which limits consumers' ability to collect and synthesize information from multiple clinicians. This simple model may be a logical starting point for a more sophisticated model.

- **Health plan- or employer-based PHRs.** These PHRs give consumers Web access to benefits information and more, based on claims data. Users can enter their medical histories in the PHR, search for providers, receive wellness education, and perform other functions.

  Again, in this model health information is tethered to one source—the health plan or employer. Consumers can get claims-based information from multiple clinicians because all claims are paid by the same payer. But they cannot access far richer clinical information, because each clinician controls the medical records in his or her possession. Amid the transition to electronic formats, health plans are creating the capacity to gather and store not only claims data but also clinical information that both providers and patients generate, including information about medications and lab results.

- **Regional health information organizations and health information exchanges.** RHIOs and HIEs are relatively new developments. They involve the creation of an intermediary entity that develops and implements policies, procedures, and systems to support the business, technological, legal, and governance infrastructures for health information exchange among health care constituents. These models are attractive because they consolidate clinical information from multiple sources.

  Unfortunately, the vast majority of RHIOs and HIEs have struggled to define a workable business model. Many of the early efforts have focused on information exchange among providers for treatment purposes rather than on giving consumers more access to and control of their personal information.

- **Internet-based products.** Internet companies are developing products that not only give consumers Web access to general information about medical conditions, illnesses, and treatments, but also offer a directory of patient-reviewed physicians. Some new products help consumers collect and store their personal health information, with the goal of ultimately enabling them to share it with care providers. This model is consumer-centric in the sense that health information is collected and stored independently of an individual's relationship with any particular clinician, health plan, or employer.

  Although Internet-based products hold great promise, they still are unproven and face significant challenges with respect to obtaining the necessary patient consents that enable the collection, storage, and use of health information in a central location.

- **Health data bank.** This emerging, though still largely theoretical, model provides a new, legislatively

authorized framework that allows consumers to store health information in a neutral, "community-owned" entity. The entity shares personal information with health care providers at the patient's discretion.

Multiple bills have been introduced in Congress that promote health data banks, which give patients ownership of their electronic records and will serve as the foundation for national health information exchange.[4]

Technological and Legal Hurdles

From a consumer perspective, all of the models described above face significant challenges.

Provider- and health plan/employer-based PHRs give consumers only slices of their relevant health information because the PHRs generally have limited ability to collect clinically rich information from multiple clinicians. Or they depend on claims information, which is less reliable and less clinically valuable. Moreover, consumer attitudes about sharing personal health information with health plans or employers, and providers' reluctance to share information with competitors, often make it difficult to create a comprehensive medical record organized around the patient.

More independent models, such as RHIOs and HIEs, solve competitive issues that have stymied the marketplace. However, there are no standards for collecting, storing, and using health information; state laws that govern access, control, and use of information vary; current laws do not give consumers any rights to access electronically generated information about their health; and RHIOs and HIEs are unregulated because they fall outside the purview of federal and state confidentiality laws. Because of confidentiality concerns, winning patients' trust can be especially difficult.

Together, the custodial models constitute a fractured, chaotic landscape that acts as an obstacle to consumer-centric health care.

Additionally, these models rely on clinicians' adoption of new electronic systems. Adoption has been slow even though the benefits of such systems are clear and widely acknowledged. One of the many reasons for the slow pace of adoption is the lack of a legally sanctioned—and operationally and financially feasible—structure for consolidating information in a way that is meaningful and useful for both clinicians and consumers.

Laws Governing Personal Health Information

Current laws and regulations governing the collection and exchange of health information have developed in an isolated, paper-based system in which providers and payers are the primary keepers of information. Consumers' access to and control of it are a secondary consideration.

Federal and state laws assume that health information must be protected under the dominion and control of health care providers and of payers who make use of selected information to pay claims, ensure quality, and operate care management programs. These laws generally do not distinguish between providers' medical records and patients' personal health information.

Providers must maintain medical records in accordance with specific standards under federal and often state laws. The records play an important role not only in patient care, but also in quality monitoring, malpractice, and other issues. Patients do not own their medical records or have an absolute right to alter them; for the most part, their rights are limited to getting copies of information in the records.

This system falls short as a viable legal framework for health information custodians, for two reasons:

1. Federal and state health care laws generally cover only certain types of entities (primarily providers and payers), so there are no parameters for how and with whom third parties—that is, entities not governed

by federal or state law — may collect and exchange personal health information. Without regulatory protection, such entities face enormous challenges in earning patients' trust.

2. Consumers have only limited rights to access, use, and control their health information. Although they do have the right to receive copies of their paper records, and federal guidance has indicated that efforts should be made to provide information electronically when it is available in that format, the laws do not include a clear consumer right to access electronic personal health information kept by "covered entities" — namely, health care providers and health plans.[6] Nor do the laws address electronic information exchange.

These regulatory inadequacies, if not corrected, are likely to limit opportunities in the emerging market for consumer-driven health information exchange.

Federal and State Laws Vary

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 governs federal regulation of health care information. HIPAA seeks to ensure that personal health information in the possession of providers and payers is protected from uses or disclosures that would compromise the interests of patients. Its reach is explicitly limited to covered entities.[6]

HIPAA regulates protected health information that third parties use for or on behalf of covered entities, based on business associate agreements between covered entities and third parties. These agreements require associates to comply with HIPAA. However, if information is transmitted to a third party that is neither a covered entity nor a business associate of a covered entity, HIPAA does not regulate it. In this case, the information is protected only under the third party's terms of use, privacy policy, or other commitments it may have made to the consumer in a data-sharing agreement. Enforcement of such agreements currently falls under general consumer protection laws rather than privacy laws.

Many states, including California, have extensive laws governing health information privacy and security. These laws often predate HIPAA and typically include more stringent restrictions on information disclosure and use. For example, California law includes special protections for HIV/AIDS testing and other specific types of particularly sensitive health information.[7] Because HIPAA does not preempt more stringent state law, these requirements are layered on top of HIPAA provisions, effectively raising the bar on legal protections for certain types of information or entities.

New York's law is structured more around the type of entity than the information it possesses. Confidentiality requirements are scattered among statutes and regulations governing various categories of providers, professions, and health plans. Thus, mental health information kept by an entity licensed by the state Office of Mental Health has greater protection, while such information stemming from a visit to a primary care physician does not.

The California Confidentiality of Medical Information Act is less fragmented and more far-reaching than HIPAA or laws in many other states. It governs not only providers and payers, but also employers. The law defines "provider" broadly to include any corporation organized for the primary purpose of maintaining medical information in order to make it available to patients or providers for diagnosis or treatment. In addition, the law covers health information that any entity obtains from other, specifically regulated entities.[8]

Despite the California law's broad reach, it regulates only entities that primarily maintain or transmit medical information. If the chain of information possession breaks down, so does legal protection. Entities for whom health information is not a primary business, and entities that obtain information from others for whom health

information is not a primary business, are not regulated by this law. In the context of personal health information custodians, this means it is possible—even likely—that some custodian models would fall wholly outside of existing regulatory authority.

An example would be an Internet service company that launches an online product to which consumers submit copies of their medical records. The company records, organizes, and posts the information on a secure Web site for each consumer's private use. Because consumers, rather than the company, have obtained this information, the chain of possession guaranteeing privacy protections under California law is broken. The company and its product are unregulated, and the information is not protected by statute.

Why Consumers Have Limited Access to Their Personal Health Information

Under HIPAA and state laws, patients have the right to access their medical records directly. However, if a patient signs an authorization permitting the disclosure of records to a third party, such as a health information custodian, the provider or health plan is not obligated to comply. The authorization permits, but does not mandate, disclosure.

Furthermore, under HIPAA, covered entities may charge patients a "reasonable" fee for copying and delivering their paper health records.[9] In California, this fee is 25 cents per hard-copy page or 50 cents per microfilm page.[10] Federal and state laws recognize that manual copying is labor-intensive.

Such fees are expensive or even prohibitive for some patients. In contrast, if electronic transactions were technically feasible and appropriate policies were in place, providers could quickly and efficiently download personal health information and transmit it to patients with the click of a button.

An electronically enabled world would not necessarily make access to health information cost free, as data providers would still incur expenses and have to charge patients a reasonable fee. But it could make access less expensive and, equally important, more convenient for patients. They would be able to receive, organize, and transmit their information more quickly and easily, enabling more timely delivery of health care.

Policymakers largely overlook the concept of a consumer right to electronic health information. Even the Health Information Privacy and Security Act,[11] recently introduced in the U.S. Senate, seeks only to establish a federal right to copy one's health records. With the exception of guidance under HIPAA privacy rules indicating that efforts should be made to provide electronic information to consumers when it is available, no current laws grant them the right to receive such information.

Toward a New Legal Framework

The number and nature of the challenges outlined here argue that a new legal framework is necessary to promote consumers' access to and use of electronic personal health information—one that also protects the information and thereby earns consumers' trust. To ensure continuity and consistency, and to facilitate the development of a consumer-centric approach everywhere, a federal framework might be best.

However, many privacy rights are embedded in state laws, and Congress has been reluctant to preempt what has long been the province of states. If state laws continue to play the central role in regulating consumer health privacy and consent, states may have to lead the reform effort. Although a state approach creates near term challenges for a national market of personal health information custodians, over time regulation could be coordinated through multi-state compacts or federal legislation.

The following policy considerations will be crucial to the success of a new, consumer-centric legal framework for personal health information.

Defining "Personal Health Information Custodian"

The first step in building a new legal framework would be to define the key features of entities that qualify as personal health information custodians in a way that includes the entire range of models. Defining custodians by their functions (for example, as clearinghouses or health information exchanges) rather than by type (provider, payer, or employer), tax status (nonprofit or for-profit), or technical or business model would increase the likelihood that, as these entities evolve, the law will remain effective.

The proposed Health Information Privacy and Security Act reflects such evolutionary flexibility. It defines a data broker as:

> "…a data bank, data warehouse, information clearinghouse, record locator system, or other business entity, which for monetary fees, dues, or on a cooperative nonprofit basis, engages in the practice of accessing, collecting, maintaining, modifying, storing, recording, transmitting, destroying, or otherwise using or disclosing the protected health information of individuals. Any person maintaining protected health information for the purposes of making such information available to the individual or the health care provider, including persons furnishing free or paid personal health records, electronic health records, electronic medical records, and related products and services, shall be deemed to be a data broker subject to the requirements of this Act."[12]

Custodians' Obligations

One issue is whether custodians would be subject to new consumer protection laws ensuring the privacy and security of personal health information and preventing its misuse by bad actors. Such laws would govern the sharing and sale of data; require meaningful consumer consent processes, transparency, data security, and protections against breaches of law or contract; and include violation remedies to help consumers feel comfortable with commercial practices.

Ideally, consent policies would ensure that consumers understand precisely what information is being conveyed by health care providers to custodians, to whom and under what circumstances a custodian may release it, and what happens to the information when a consumer's relationship with a custodian ends.

Providers' and Payers' Obligations

Meaningful consumer rights to standardized, electronic personal health information would give consumers enforceable authority to direct a clinician, a payer, or any entity holding such information to send a copy of it to the personal health information custodian of the consumer's choice. This is essential because many consumers may not have the desire, capability, or necessary security protections to store and use the information on their home computers.

Legally binding rights would also update the fees that holders of personal health information could charge for transmitting it electronically. One challenge will be the limited capability of most clinicians to share electronically formatted information with patients or their representatives.

Importantly, new laws would need to allow sufficient time for the market to adapt. In the absence of mandates, however, providers and others may find little incentive to make access to electronic health information an affordable option for consumers.

Economic Incentives for Physicians

To be of value to consumers, electronic personal health information must be available in a format that makes

it easy to combine information from multiple sources and organize it in a comprehensible way. A variety of incentives for clinicians are emerging that encourage them to install and use electronic health records to improve consumers' overall health. The incentives often are conditioned on compliance with national standards.

Significantly less attention has been paid to the capability of technology systems to electronically convey health information to consumers. Linking physician incentives to such capability would accelerate consumers' engagement in their health care and the potential clinical benefits that could result.

Incentives might include state or federal grants and specific Medicaid and/or Medicare reimbursements. Over time, government policy could evolve to include stronger mechanisms for ensuring that standardized personal health information is transmitted electronically—for example, by making this capability a condition of participation in Medicaid, Medicare, or other government-financed health programs.

Enforcement Is Essential

Enforcement of new, consumer-centric laws would likely be essential to ensure compliance. Without clearly defined legal protections that are enforced, consumers will be reluctant to entrust their personal health information to third parties. Enforcement would protect information custodians as well as consumers.

Conclusion

As adoption of health information technology and the ability to exchange personal health information advance, so too should the legal foundation that facilitates access to and control of such information for consumers' benefit. Early technological advances offer a window of opportunity to design legal parameters for appropriate consumer access and control, regardless of the information's source or how it is used.

At a minimum, new laws should give consumers an affirmative right to authorize the transmission of any standardized, electronic personal health information to a custodian of their choice, and ensure that custodians use such information in a manner directed by consumers. These laws would have significant potential to engage patients in their health care by clearly defining their rights (thus winning their trust) and fostering models of information custodianship that support their needs.

Authors

William S. Bernstein, J.D., Julie V. Murchinson, M.B.A., Melinda J. Dutton, J.D., Terri D. Keville, J.D., and Robert D. Belfort, J.D.; Manatt Health Solutions

Acknowledgment

Special thanks to those who also contributed to this publication including JanLori Goldman, David Lansky, Kalpana Bhandarkar, Lori Evans, Lucia Savage, and Rachel Block.

About the Foundation

The California HealthCare Foundation, based in Oakland, is an independent philanthropy committed to improving California's health care delivery and financing systems. Formed in 1996, our goal is to ensure that all Californians have access to affordable, quality health care. For more information about the foundation, visit us online at www.chcf.org.

Endnotes

1. California Health and Safety Code § 123110(b).
2. Markle Foundation. Americans Want Benefits of Personal Health Records. June 2003 (www.connectingforhealth.org/resources/phwg_survey_6.5.03.pdf).
3. Notable among these activities is the Markle Foundation's Connecting for Health Work Group on Consumer Access Policies.
4. See, for example, the Independent Health Record Bank Act of 2006, H.R. 5559/S. 3454, which did not become law. It proposed limiting data banks to nonprofit organizations and specified that such entities would be considered covered entities under HIPAA (www.govtrack.us/congress/billtext.xpd?bill=h109-5559 and www.govtrack.us/congress/billtext.xpd?bill=s109-3454). See also the Health Record Trust Act, H.R. 2991, introduced in the House of Representatives in July 2007 (www.govtrack.us/congress/billtext.xpd?bill=h110-2991). See also (1) Yasnoff, W.A. HRBA: Health Record Banking Alliance (www.hhs.gov/healthit/ahic/materials/06_07/cps/hrba.pdf); (2) Ibid. "Health Record Banks Enable Privacy in Health Information Infrastructure." Presentation to NCVHS Privacy and Confidentiality Subcommittee, Hyattsville, Maryland, January 23, 2007 (www.ncvhs.hhs.gov/070123p2.pdf). In this model, the multi-stakeholder board of a nonprofit data bank would regulate privacy.
5. Goldman, J. "New consumer right fuels opportunity for e-access to medical records." iHealthBeat, October 30, 2002 (www.ihealthbeat.org/articles/2002/10/30/New-consumer-right-fuels-opportunity-for-eaccess-to-medical-records.aspx?ps=1&authorid=).
6. 45 Code of Federal Regulations. § 160.102. HIPAA also covers "health care clearinghouses," narrowly defined as entities that translate data from nonstandard to standard format.
7. California Health and Safety Code §§ 120975.
8. California Civil Code Sections 56–56.16.
9. 45 Code of Federal Regulations. 164.524(c).
10. California Health and Safety Code § 123110(a) and (b).
11. The text of this legislation is available at www.govtrack.us/congress/billtext.xpd?bill=s110-1814.
12. Ibid.