Jumpstarting Access to Personal Information with Rights-based Legislation

by William Bernstein, JD

Providing consumers access to their health information seems like a simple concept. In reality, it is fraught with challenges. Records are still largely in paper form, and gaining access to them means contacting multiple parties and paying significant fees. Even when records are in electronic form, there is no easily accessible place where individuals can store them in a secure environment.

Nor are sufficient legal safeguards in place to ensure consumers have control over the way this information is used. At present, a morass of highly variable company policies and fineprint privacy clauses govern consumers' rights, rather than a well-defined federal or state policy framework.

It is not hard to imagine how access and protection could work in an ideal, electronic healthcare system. Health IT could enable consumers to easily transmit either discrete portions or comprehensive files of their data to caregivers on demand and in a matter of seconds. They could access personal information from various sources, search for data that are useful for care decisions, store the information in one location, organize it in formats that are meaningful to themselves and their providers, and access educational features that help them participate in their care.

But to successfully transform consumers' ability to access and use their health information, there must be significant change in the laws that govern health information. Having a right to information is only meaningful if the information can be obtained in an affordable and timely manner.

The legal system currently is designed to protect unauthorized disclosures of patient records by a provider or payer. It must change to one that provides consumers with a meaningful right to gain access to their own information and control its use.

Currently: An Inadequate Legal Framework

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

Federal and state laws are structured so that health information is protected under the dominion and control of healthcare providers and payers. These laws generally do not distinguish between providers' medical records and patients' personal health information.

Under HIPAA and state laws, consumers do not possess a meaningful right to access their personal health information. For the most part, their rights are limited to getting copies of information in their records on terms that are often expensive, laborious, and subject to delay.

For business, legal, and clinical reasons, provider organizations create and manage patient medical records, and patients do not have an absolute right to alter them. However, the inability to easily access their personal information is believed by many to make it more difficult for patients to participate effectively in making informed decisions about their own healthcare.

In addition, HIPAA does not preempt state law. Thus federal and state statutes and regulations around privacy of personal health information and consumer access to it vary. Some state laws place significantly more stringent restrictions on information disclosure and use than does HIPAA; further complicating the legal landscape, these restrictions vary between states. Additionally, confidentiality requirements are scattered across multiple sections of code within states themselves, creating even more fragmentation and potential for confusion.

Fees for the transmission of electronic health information also vary considerably by state. HIPAA simply provides that covered entities may charge a "reasonable fee," while state laws set prices at what can amount to very high fees, such as California's law allowing that consumers may be charged up to 25 cents per page.

Why a New Framework Is Needed

Changing our laws to legally sanction and define the role and responsibilities of "personal health information custodians" would fundamentally change today's existing paradigm.

In effect, this new breed of "authorized agent"—whether it be an Internet service company, a health plan, a provider entity, or a newly created company—would assist patients in obtaining, organizing, and using their health information. Agents would perform for consumers the task of collecting healthcare information from multiple sources and organizing it in a manner that would make it useful, such as allowing patients to track their medical histories, easily seek second opinions, share information with caregivers or family members, and research specific health issues.

It might be argued that personal healthcare custodians can exist today, without any change in law, by obtaining patient consent to have information sent to them and entering into agreements with patients as to how such information is organized and used. While this is true, the current approach places a large responsibility on the consumer to understand different company policies, and it ultimately provides very little protection against misleading or deceptive practices.

Moreover, new laws recognizing personal healthcare custodians as authorized agents of patients could accelerate consumer access to personal health information by defining the terms upon which health information is transferred—price, speed, data standards, and formats—in ways that help overcome current barriers to consumer access.

Just as significantly, consumers need to know that personal health information custodians acting on their behalf will carry out their functions in a way that ensures the privacy and security of patients' health information. None of us are experts on the best way to keep our information private and secure, and we all know from experience about the dangers of signing long agreements with lots of fineprint. In order for personal healthcare custodians to gain consumers' trust, they must agree to carry out their roles in ways that guarantee consumers basic protections against the misuse of information.

Working toward a Solution: A New Statutory Framework

What is required for change is a new statutory framework that defines the role "personal health information custodian," affirmatively requires providers and payers to transmit healthcare information to such custodians in a timely and affordable manner, and ensures consumers that such information once transferred will be subject to basic consumer protection principles.

While ideally the change would come through a federal statute that preempted state laws, state-level solutions will likely be most achievable in the short term, and they could create a foundation for the eventual changes in federal law.

Change will first require the building of a broad-based coalition of interested stakeholders within each state who are united in support of a common set of consumer empowerment and privacy protection principles. This coalition would come together to draft model legislation. Draft legislation must be tailored to each state's regulatory context, but must also contain several common elements. These elements include:

A clear definition of "personal health information custodian." New laws must clearly define the key features of entities that will qualify as personal health information custodians. Defining custodians by their functions (such 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, will help ensure that the law remains effective as these entities evolve.

The starting point for such a definition might be drawn from the proposed Health Information Privacy and Security Act, introduced to the Committee on Health, Education, Labor, and Pensions by Senator Patrick Leahy in 2007. 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."

An affirmative right to consumer access in an affordable and timely manner. New laws must create an explicit right for consumers to be able to access, send, and store their electronic information as they see fit. The law must require that providers and payers comply with consumer requests to have their personal health information sent electronically to the custodian of their choice.

Laws should also set the price of fees that holders of personal health information could charge for electronically transmitting the data to patients or to their chosen data custodian. States might additionally consider mandating that electronic information be available using state-approved data standards and formats. Of course, such new laws would apply only to providers who have adopted electronic health records.

A strong consumer protection framework. New laws must include safeguards under consumer protection laws to ensure that information is secure and used appropriately. These protections should govern the sharing and sale of data and require meaningful consumer consent processes, data security, and protections against breaches of law or contract.

The laws should include penalties for entities that violate these regulations. Ideal consent policies would facilitate informed consumer consent by ensuring that patients understand exactly what information is being disclosed to custodians, to whom and under what circumstances a custodian may release that information, and what happens to the information when a consumer's relationship with the custodian ends.

Notably, legislation alone will not suffice. Advocates of a personal health information custodian model must also demonstrate that there is a sustainable business model that supports greater consumer use of health information. As this market matures, we will learn much about the actual business case for greater consumer involvement in healthcare decision making.

New legislation also needs to be coupled with the establishment of strong enforcement provisions, particularly relating to such issues as deceptive consumer marketing practices and security breaches, in order to engender consumer trust and protect both information custodians and consumers alike.

Yet, while legislation alone is not sufficient, it is a necessary starting point. By establishing that consumers have a meaningful right to access and use their own electronic health information and the principal terms upon which such access must be granted, the healthcare market will be required to respond to consumer demands to control and use their own health information.

Consumer access legislation can thus jumpstart our efforts to move closer to realizing the potential of an electronically enabled and consumer-centric healthcare system.

Reference

Bernstein, William S., et al. "Whose Data Is It Anyway? Expanding Consumer Control over Personal Health Information." California HealthCare Foundation. February 2008. Available online at www.chcf.org.

William Bernstein (wbernstein@manatt.com) is chair of the healthcare division of Manatt, Phelps & Phillips in New York, NY.

Article citation:
Bernstein, William. "Jumpstarting Access to Personal Information with Rights-based Legislation" *Journal of AHIMA* 79, no.7 (July 2008): 54-55;61.