Privacy and Health Information Exchange—in an Ideal World and a Real World

Linda Ackerman, Staff Counsel
PrivacyActivism
lga@privacyactivism.org

Introduction

The debate about information privacy is relatively recent and is largely a consequence of the explosion of online content, including the collection of personal information into vast databases controlled by the government or commercial data brokers. Paper-based information was obscure and difficult to obtain. Digital information is ubiquitous, readily available and eternal.

Now we come to the point where there's an executive mandate to make personal health information electronic and universally available. The purpose of the effort is to improve the quality of health care in the U.S. while lowering the costs. There will also be many unintended consequences of health information exchange—good and bad.

What's essential, though, is that no system or piece of a system be put into place without taking into account the need to protect the privacy and security of health information from the very beginning.

1. Why should personal medical information be private?

a. Almost all medical information is inherently sensitive. For example, the prescriptions you're taking reveal a great deal about your medical conditions—including mental health status—that you may simply want to keep to yourself. This would be true even without references to possible consequences of disclosure—just based on the conviction that it's no one's business but yours.

b. What about the consequences of disclosure? I think few people would object to the sharing of medical information among various providers for the purpose of treatment. The argument is made that your podiatrist doesn't need to see your gynecology records, but I disagree. For one thing it would discourage even further any holistic approach to health care—in the sense of treating the whole person and not just the part that belongs to the specialist you're seeing. For another, you could be putting yourself at risk of adverse drug reactions if one doctor doesn't know what another one has prescribed.

   Other types of disclosure should not be allowed, at all—such as disclosures of medical treatment or conditions, or mental health status—to employers, non-health insurers, financial institutions—to any business or organization where your medical information could or would be used against you, or even just to market to you.

2. Privacy and health information exchange

Privacy is an essential piece of the foundation of any successful National Health Information Network.

The ambitious and admirable goals of the NHIN are to improve the quality of health care, deliver health care more efficiently and cut the cost of care.

(a) COST

Clearly, it is critical to get a grip on the cost of health care. The statistics are from the National Coalition on Health Care:

(1) Total spending was $2 TRILLION in 2005, $6,700 per person, or 16 percent of the gross domestic product (GDP). Spending is expected to reach $4 TRILLION in 2015, or 20 percent of GDP. Keep in mind that as we continue to spend incomprehensible amounts of money on health care, close to 15% of the population has no coverage at all and either goes without or resorts to emergency rooms, which increases the overall cost for everyone.

(2) In 2006, employer health insurance premiums increased by 7.7 percent – two times the rate of inflation. The annual premium for an employer health plan covering a family of four averaged nearly $11,500. The annual premium for single coverage averaged over $4,200

One obvious result of out of control costs is that health insurance is a hot potato, with everyone trying to shift the burden elsewhere. Most of the increases are absorbed by consumers. The government cuts its costs by decreasing eligibility and eliminating certain types of care from coverage.

Getting cost under control is an important reason why HIE and the NHIN have to succeed. But for that to happen, there are strong indications that consumers will have to be satisfied that the privacy of their medical information is not just respected but legally protected.

(b) QUALITY OF CARE

Surveys also show that consumer attitudes about privacy will seriously impact the NHIN's goal of improving the quality of care:

- Dr. Alan Westin presented results of a survey in a presentation titled "How the Public Health Views Health Care, Privacy and Information**,"** to the National Committee on Vital and Health Statistics (NCVHS—the public advisory body to the Secretary of HHS). He found that 65% of those he surveyed would not disclose information to their provider because they worried it would go into computerized records. (See http://ncvhs.hhs.gov/050223tr.htm#westin)

- A January 2000 California HealthCare Foundation survey, titled "Ethics Survey of Consumer Attitudes about Health Web Sites," found that 75% of Americans are concerned about the loss of medical privacy due to the use of an electronic health and information system. (See http://www.chcf.org/topics/view.cfm?itemID=12493)

3. The role of privacy at the beginning of the HIPAA process.

The department of Health and Human Services (HHS), which administers the National Health Information Network (NHIN) through the Office of the National Coordinator (ONC—formerly the Office of the National Coordinator for Heath Information Technology), seems to have understood the importance of privacy to the success of health information exchange HIE at one point. In an HHS Federal Register Notice on "Standards for Privacy of Individually Identifiable Health Information," December 28, 2000; 65 Federal Register 82462-82467, the department advocated for privacy protective standards for medical information as being fundamentally necessary for consumer acceptance of sharing of electronic records:

> "[T]he entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers."
>
> "While privacy is one of the key values on which our society is built, it is more than an end in itself. It is also necessary for the effective delivery of health care, both to individuals and to populations."
>
> "Unless public fears are allayed, we will be unable to attain the full benefits of electronic technologies. The absence of national standards for the confidentiality of health information has made the health care industry and the population in general uncomfortable about this primarily financially driven expansion in the use of electronic data."

From that recognition of privacy as a key factor in the development of a NHIN, we go to the standards that eventually resulted—the HIPAA privacy regulations.

4. The current state of HIPAA privacy protection

There are those who describe the HIPAA regulations as privacy protective. In my view, HIPAA is not a privacy rule but a disclosure rule. Nothing makes this clearer than a timeline put together by Dr. Deborah Peel, the founder of an organization called Patient Privacy Rights (www.patientprivacyrights.org):

1996 Congress passed HIPAA, and instructed the Dept. of Health and Human Services (HHS) to address the rights of patients to privacy. The following sections from Public Law 104-191, the Health Insurance Portability and Accountability Act, express the intent of Congress with regard to privacy.

Sec. 264 (a) The recommendations under subsection (a) shall address at least the following:

> Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit to [Congress]…detailed recommendations on standards with respect to the privacy of individually identifiable health information."

Sec. 264 (b) The recommendations under subsection (a) shall address at least the following:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required

2001 President Bush implemented the original HIPAA "Privacy Rule" recognizing the "right of consent."

HHS promulgated "Standards for Privacy of Individually Identifiable Health Information" (i.e., "the Privacy Rule") 65 Fed. Reg. 82,462. As you can see, individual consent was required for disclosure of protected information.

"….a covered health care provider must obtain the individual's consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations."

Just to make it clear that Congress had privacy in mind and believed that it was key to the success of HIE, a few more quotes from the preamble to the Standards for Privacy laid out in the Federal Register:

- Congress has long recognized the need for protection of health information generally, as well as the privacy implications of electronic data interchange and the increased ease of transmitting and sharing individually identifiable health information." 65 Fed. Reg. at 82,469
- [The] growing [public] concern [about the loss of privacy] stems from several trends, including the growing use of interconnected electronic media for business and personal activities, our increasing ability to know our genetic make-up, and, in health care, the increasing complexity of the system." 65 Fed. Reg. At 82,465
- [F]ew experiences are as fundamental to liberty and autonomy as maintaining control over when, how, to whom, and where you disclose personal material." 65 Fed. Reg. at 82,464-65

- The electronic information revolution is transforming the recording of health information so that the disclosure of information may require only the push of a button. In a matter of seconds, a person's most profoundly private information can be shared with hundreds, thousands, even millions of individuals and organizations at a time." 65 Fed. Reg. at 82,464-65
- The right of privacy is: 'the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated.'" 65 Fed. Reg. at 82,465
- Comments from individuals revealed a common belief that, today, people must be asked their permission before each and every release of their health information" 65 Fed. Reg. at 82,472
- Citizens "have strong expectations regarding consent for use and disclosure of health information." 65 Fed. Reg. At 82,473

2003 Amendments to the "Privacy Rule" became effective, eliminating patients' "right of consent," overruling the expressed intentions of Congress and the President, and turning HIPAA into a disclosure law:

"The consent provisions…are replaced with a new provision…that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations." 67 Federal Register at 53,211

Regulatory permission means presumptive rather than individualized consent, with or without notice, over a patient's objection and even if an individual pays privately and no government or private insurance is involved. In other words, it is a rule that mandates disclosure regardless of consent.

Other serious shortcomings of the amended HIPAA rule include:

- Citizens "have strong expectations regarding consent for use and disclosure of health information." 65 Fed. Reg. At 82,473
- Such privacy protections as there are apply only to "covered entities."
- There's no requirement for a covered entity to notify individuals in the event of a data security breach.
- Covered entities are not required to account for routine disclosures for "treatment, payment and operations" (TPO).
- Enforcement is extremely weak. Of the more than 30,000 complaints received by the Office of Civil Rights (OCR) since the HIPAA rules went into effect in April 2003, there have been only two prosecutions.
- There is no private right of action for individuals to sue for an alleged HIPAA violation, only an administrative process that is notably ineffective

in achieving redress.

In terms of regulations, judicial decisions and the policy of the current Department of Justice, this is where we are now—as the process of electronic exchange of health information progresses toward fruition:

- Federal Court Findings – Citizens for Health v. Leavitt (03-2267 E.D. PA)

  Federal District Court Judge Mary McLaughlin: "It is true that providers are permitted by the [HIPAA] Rule to seek consent before disclosing [plaintiffs'] health information. They have chosen not to do so…..the Amended Rule has a sufficiently determinative and coercive effect on the action of the providers ….The Amended Rule has changed the landscape established by the Original Rule in which decisions will be made by providers as to whether they will seek consent or agree to patients' demands for consent."

- Dept. of Justice position in the Oral Argument, in Citizens for Health v. Leavitt (U.S. Court of Appeals for the Third Circuit, March 9 ,2005):

  In response to question from the Court regarding whether, under the HIPAA Amended Privacy Rule, patients may refuse to allow their identifiable health information to be used and disclosed: "…the short answer is you never had a right to absolutely prevent information that was necessary for the core functions of the healthcare system to operate from being disclosed to an insurer." Transcript of oral argument at 21.

  "Patients no longer possess a reasonable expectation that their medical histories will remain completely confidential."

- Dept. of Justices position in 2004 regarding cases seeking to compel disclosure of medical records of women who had received abortions:

  Federal law "does not recognize a physician-patient privilege...[patients] "no longer possess a reasonable expectation that their histories will remain completely confidential". In other words, under DOJ policy, there is no protection of confidential medical information from mere political agendas.

5. The ideal resolution for privacy of medical information

(a) Recognize a right to the privacy of medical information, as defined in the June 22, 2006 Report of the NCVHS to HHS Secretary Leavitt: "Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data." ("Recommendations Regarding Privacy and Security in the National Health Information Network," NCVHS letter to DHS Secretary Leavitt; http://www.ncvhs.hhs.gov/060622lt.htm)

This definition includes accessible user interfaces, so that disabled health consumers can individually manage their health records to ensure their medical privacy.

(b) The right to medical privacy applies to all health information regardless of the source, the form it is in, or who handles it.

(c) Some believe there should be a right to opt in or out of electronic health exchange, but don't think it's possible to have a less than universally inclusive system and still achieve the goals of the NHIN—that is, improving the quality and delivery of care, while reducing the cost.

(d) There should be a right to segment or exclude certain information on a "need to know" basis, but direct providers of health care should not be prevented from seeing anything less than a patient's entire record. This means anyone directly involved in treatment, and should certainly include doctors and nurses, with room to debate whether those who merely administer diagnostic tests also qualify, or should fall into a "minimum necessary" category.

(e) Patients should exercise control over access to their electronic health records to the extent of being able to restrict or deny access for non-treatment purposes. This would include denying access to employers, financial institutions, non-health insurers—anyone whose interest is unrelated to actual medical treatment.

(f) Health information disclosed for one purpose may not be used for another purpose without informed consent, preferably written.

(g) Disclosures of patient information should be auditable in real time.

(h) Patients should be notified promptly of suspected or actual security breaches, without splitting hairs about whether or not there is a risk to an individual from a disclosure—as is the case with the California breach notification law (CA Civil Code §1798.29).

(i) Ensure that consumers can not be compelled to share health information to obtain employment, insurance, credit, or admission to schools, unless required by statute

(j) Preserve stronger privacy protections in state laws. In other words, no federal pre-emption of state laws.

(k) No secret health databases. Require all existing holders of health information to disclose if they hold a patient's health information. This would include providers—public and private, insurers, prescription databases, the MIB database, and even quasi-medical information held by data brokers and used for targeted marketing to pregnant women or new mothers. Individuals should be able to request expungement of their medical information.

(l) Provide meaningful penalties and enforcement mechanisms for privacy violations detected by patients, advocates, and government regulators, including a private right of action.

6. What kinds of privacy and security protections can consumers reasonably expect in a National Health Information Network, or any system of electronic health information exchange?

   (a) We can make the NCVHS definition of health information privacy a reality: "Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data." Again, I would make treatment the exception to individual control.

   (b) Use of information for the purpose it was collected is essential. Medical data is extremely valuable to a variety of interests—legitimate, criminal, known or yet to be imagined—but it should not be used, even in an allegedly "de-identified" form, for anything, including research without express, preferably written, consent.

   (c) Maintaining data quality should be the shared responsibility of the providers who generate the information contained in a medical record and the person whose record it is. This presumes individual access to records and the ability to annotate whatever the record subject believes is incorrect. The provider or diagnostic service that created the information should be required to verify and correct if necessary. This goes to the heart of the reasons for having a system of health information exchange in the first place: incorrect data obviously affects the quality of care.

   (d) Individuals have a right to know who holds their data. I don't know the technological solution for this requirement, but I believe it's important to find one.

   (e) No coerced sharing of medical information. That is, no one should be required to reveal their medical information as a prerequisite for a job—unless, for example, one is applying to be an astronaut—or in order to qualify for a mortgage.

   (f) There should be serious penalties for abuse of medical information and a private right of action so that individuals can pursue their own claims.