Who Should Have Access to Your Information? Privacy through the Ethics Lens

by Emily Friedman

How can HIM professionals balance the data demands of outside parties with the patient's assumption that health information will be kept private? The author examines this question through the lens of ethics.

And yet, and yet, one thing I keep from you...."

—Ella Wheeler Wilcox

More than 150 years ago, Alexis de Tocqueville, a French political scientist who had come to the United States to study our prison system, made a telling observation about our politics and culture.

He wrote that the basic conflict at the heart of our democracy was the one between the individual and society—between the rights of the person and the rights of the community at large. He suggested that this conflict might never be solved. Nearly two centuries later, de Tocqueville is still considered one of the most sage observers of Americans who ever lived.

As he noted, the fact is that most of us, in and out of healthcare, have two lives, particularly when it comes to personal information: one life that seeks data and information and even gossip about celebrities, neighbors, and (sadly) patients and colleagues, and another life that demands that personal information about oneself, especially health information, be kept as secret and sacrosanct as the launch codes for nuclear missiles—perhaps more so.

And so the question must be asked: in this environment, can these two lives be reconciled? How can the HIM professional balance the data demands of outside entities with the patient's, or insured person's, or employee's assumption that his or her personal health information will be protected?

There are many ways in which this question can be answered: Legal. Regulatory. Professional. Practical. Logistical. Market. Financial. But there is one other consideration, and that is the ethical and moral one. The question it asks is one of rights, of just who has an ethical or moral right of access to personal healthcare information—and to what end?

Information: Yours, Mine, and Ours

Every entity that claims a right of access can come up with a well-framed and persuasive argument as to why it should have such access.

Physicians, hospitals, and other care providers, of course, argue that they should have access to the medical records and other health information of any patient at any time because they need this information to provide the best possible treatment, to learn of drug interactions and allergies and other existing risks, and to avoid reinventing the wheel in terms of planning treatment. These are valid arguments.

Insurers claim that they must have personal health information in order to properly process claims and pay for care, in addition to protecting against fraud by providers or patients or families. These are valid arguments.

The federal government—representing Medicare, Medicaid, and other programs—makes many of the same arguments as insurers, saying that, in providing taxpayer-funded coverage to more than 70 million Americans, it has the right to know what it is paying for and to protect against fraud and abuse. These are valid arguments.

Researchers, both clinical and nonclinical, argue that they need access to personal medical information to improve the quality of care, to protect patients against improper or even dangerous care, and to conduct studies that will make healthcare more effective and produce new products and therapies. These are valid arguments.

As a matter of fact, just about everyone can make a claim that he, she, they, or it has a right to get into other people's medical records because of what they want to do—to improve clinical healthcare or the performance of the healthcare system or the effectiveness of health coverage or to further some other goal.

The only people, in fact, who seem to be without a voice in this clamor to be exempted from privacy protections (such as they are, and such as they are likely to be under the new federal administration) are patients: the people whose records they are, and yet who, until now, in many states, could not see for themselves the very personal information that so many others are seeking to scrutinize.1

This brings us to the three basic ethics issues that are involved with increasing public use and release of personal medical information:

• is personal healthcare and health status information a private or a public matter?

• to what uses should this information be put, especially if the result could be harmful to the patient?

• what protections and sanctions are appropriate when personal health information is misused?

The Public Looks to the Guardians at the Gate

In terms of the first question, I believe the answer is unequivocal: personal information about me, my body, and my health status is the business of me and those who take care of me. Nobody else—nobody else—should have access to that information without my freely granted and informed permission, unless the circumstances are truly extraordinary. And rarely are circumstances that extraordinary.

Beyond law, beyond payer requirements, beyond all the conveniences for non-patients that have been introduced into the recording and keeping of personal healthcare data lies a simple truth: if we, from the billionaire to the street person, own anything on this earth, it is our bodies. Indeed, bioethicist H. Tristram Engelhardt has described the human body as the ultimate personal property.

It is, therefore, absurd that a person is not allowed to see the record of what happens to one's body in its journey through the healthcare system, when many people who have no ethical right to do so can rifle through those same records like police with a search warrant.

The public's fear about improper release of personal health information is widespread, as has been shown by many recent studies. In a 2000 survey funded by the California HealthCare Foundation, 55 percent of Internet users had no problem with information about what they had purchased online being shared; 48 percent were willing to have information about what ads they had clicked shared; but only 3 percent were willing to have their personal health information shared.

Similarly, 60 percent of Americans studied by Princeton Survey Research in 2000 indicated they were unwilling to have their medical records shared with hospitals that were offering relevant preventive medicine programs; 61 percent were unwilling to have a new employer granted access to their medical records; and 70 percent were unwilling to have their records shared with pharmaceutical manufacturers, even if those manufacturers were providing information about new drugs that might help the patients.

The good news, for HIM professionals, is that patients trust healthcare providers far more than insurers or government to keep their medical information private. The bad news, of course, is that in this inquisitive environment, honoring that trust is increasingly difficult.

Nonetheless, healthcare provider organizations and their HIM professionals remain, in patients' minds, the guardians at the gate. And it is a gate that desperately needs to be guarded.

Drawing the Line

The second ethics question involved in all this is: to what uses might this information be put ethically?

There are several obviously appropriate purposes. The most compelling is when a healthcare professional is taking care of a patient, especially in an emergency or other circumstances when the patient may not be known to the provider.

Also, if an insurer—public or private—simply wants information to pay a claim, that is also appropriate. And, under certain circumstances, if researchers need information for legitimate study purposes, that information should be made available—but without personal identifiers, of course.

But when those involved in these legitimate activities make demands that seem inappropriate, the records must be protected.

There are also areas of endeavor in which the disclosure of personal medical information without patients' or families' permission or without proper informed consent must be resisted. These include:

• inappropriate press inquiries. It does not matter if it is the president of the United States or Joe Schmoe, or whether financial incentives are offered; the press has no inherent ethical right to detailed health status information about anyone without consent

• inappropriate insurer inquiries. HIPAA and many state laws require certain protections for persons in the individual and small-group insurance markets. Insurers often seek to circumvent these protections through unsanctioned obtaining of personal health status information. Besides being illegal, these activities are also unethical, resulting, as they often do, in people losing health insurance at the time they need it most

• inappropriate employer or prospective employer inquiries. These days, it is common for employers or prospective employers, especially those that are self-insured, to wish to "weed out" employees or prospective employees who might be, by reason of current or potential health status, "bad risks" in terms of health insurance. In addition to major legal questions, this practice will inevitably lead to a healthcare "underclass" that, although willing and able to work, cannot do so because of insurance concerns. The Americans with Disabilities Act was passed to prevent this sort of thing from happening, but it still happens. HIM professionals should have no part in it

All these risks are likely to be exacerbated by increasingly sophisticated techniques in detection of genetic predisposition to disease, which will, of course, become part of medical records. One does not like to think of a society, as envisioned by Aldous Huxley in Brave New World, in which only the genetically correct survive.

A Culture of Confidentiality

Finally, what protections and sanctions are appropriate when personal health information is misused? First and obviously, every effort must be made to see that such information is not allowed to get into the wrong hands to begin with. This starts with the proper technological protections, to the degree that we have such sophistication.

That needs to be accompanied by leadership from within the HIM professional ranks, especially from those who are unwilling to go along with improper policies and demands. Is this easy? Of course not. Is it risky? Of course. But if no one is willing to say "no," then the most dubious users of information will define the profession, and none of us will be safe.

Second, when there is documented evidence—and systems should have audit trails so that such evidence exists—that someone within the organization has played fast and loose with personal health information, there must be both policy and practice. Policy should consist of written and distributed documents that make it very clear that the inappropriate use or dissemination of personal health information is a firing offense.

Practice enforces that policy, and does so equally across the spectrum of healthcare workers. I was recently told the story of a hospital to which a celebrity patient was admitted. Within days, the number of internal computer "hits" on that patient's medical records was 20 times what might have been expected for an average medical record. With an audit trail, the hospital leadership was able to identify the offenders; medical privileges were suspended and people were fired.

This type of enforcement, with teeth, is a major and very visible part of the process needed to create a culture of confidentiality, by which any patient or family member may be assured that personal information remains personal.

Such a culture requires more than heroic action on the part of the HIM professional; it requires an organization-wide commitment to privacy and confidentiality as a value, as a part of day-to-day activity, as a central part of indoctrination and training, and as an accepted principle.

We aren't there yet. When the Clinton administration announced its final rules on medical privacy pursuant to HIPAA requirements in December 2000, more than one healthcare industry association immediately complained about their complexity, confusion, and cost. And just about everyone complained about being made accountable for how health information is used.

We are accountable for how health information is used; we're the ones who collect and keep it. And it is time—it is far past time—that HIM professionals started demanding that everyone else in the organizations in which they work begin to share that accountability.

Personal health information should be treated by everyone in healthcare as though it concerned themselves and their families; because the odds are that, someday, it will.

Note

1. The final regulations on privacy standards for individually identifiable health information under HIPAA released in December 2000 provide that patients may have access to their medical records; however, at press time it was unclear whether these regulations would be endorsed by the new administration.

Emily Friedman *is an independent health policy and ethics analyst based in Chicago. She can be reached at 851 W. Gunnison Street, Chicago, IL 60640.*

Article citation:
Friedman, Emily. "Who Should Have Access to Your Information: Privacy Through the Ethics Lens." *Journal of AHIMA* 72, no.3 (2001): 24-27.
