Understanding HIPAA: What It Protects and What It Permits

By Carol Levine

It is hard to keep a secret in a digital world, as celebrities and other prominent citizens have learned to their dismay. True, many people delight in sharing intimate details about their lives, from the most trivial to the most significant, on Facebook, Twitter, and other social media. In health care, some patients, especially those with rare or difficult-to-treat illnesses, maintain or contribute to websites that detail every aspect of their diagnosis and treatment. Others provide less specific updates on blogs.

Still, most patients do not want their medical information available to anyone who does not need it in order to provide, assist with, or pay for their care. They are particularly concerned that this information not be given to employers, marketers, or fundraisers. And they certainly don’t want reporters, business competitors, or nosy neighbors or coworkers to have it.

Recognizing the importance of respecting personal autonomy and dignity, ethical codes of conduct for every health care profession stress confidentiality. The National Association of Social Workers’ standards for social work case managers, for example, states: “The social work case manager shall ensure the client’s right to privacy and ensure appropriate confidentiality when information about the client is released to others” (Standard 4). The American Nurses Association has two standards: “Privacy (3.1): The nurse safeguards the patient’s right to privacy. The need for health care does not justify unwanted intrusion into the patient’s life.” This is followed by “Confidentiality (3.2): Associated with the right to privacy, the nurse has a duty to maintain confidentiality of all patient information.”

If patients and professionals agree in principle, why is privacy such a problem in health care? Part of the reason lies in the details. Who is entitled to medical information? What standards should guide disclosure? How can medical records be kept secure from hackers or careless employees? And what are the consequences of inappropriate disclosures?

These are not theoretical questions. They come up all the time in practice. Case managers are often faced with patients and families who come to them after dealing with other staff who have given them unclear, conflicting, or no information. Sometimes patients and families are being asked to make major decisions without all the relevant facts. Sometimes case managers have to weigh institutional priorities against individual needs or preferences. For case managers, then, it is essential to have a solid grounding in what the privacy law, as well as professional ethics, requires and—equally important—what they permit.

Definitions

Privacy and confidentiality are often used interchangeably, but there are differences in interpretation. Even privacy can have different meanings. One meaning relates to the person. Curtains may be drawn around a patient’s bed to protect his or her privacy while undergoing an examination. Significant discussions with patient and family may take place in a private area so that others are not able to hear. In the legal context, privacy extends from the person’s physical being to information about the person gathered in the course of medical care. Confidentiality refers to the obligation of professionals to prevent the information from being disclosed unless authorized by the patient or required by law or clinical judgment. Elevator talk about a patient, for example, is a violation of confidentiality. So is disclosure to the media that a celebrity is a hospital patient.

Disclosures may be inadvertent or deliberate; whatever the cause, they may result in harm to a person’s livelihood, reputation, or personal relationships.

In protecting privacy and assuring confidentiality, a third element—security—becomes critical. Security refers to the technical or practical measures
Regardless of the trainers’ intent, staff members who attended these sessions clearly heard the message, “If you want to be safe, don’t tell anyone anything.”

used to prevent unauthorized access, use, and dissemination. Security can be addressed by policies that restrict access to information, safe storage, and limits on employees’ off-site use of information, as well as by electronic systems that encrypt information.

What HIPAA (and Now HITECH) Cover
The federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, known as HIPAA) and the Privacy Rule of 2003 (45 C.F.R, 164.510[b], the regulation implementing HIPAA) form the legal basis of safeguarding protected health information (PHI). Before HIPAA, confidentiality of medical information was covered by a patchwork of state laws and regulations that sometimes conflicted and certainly confused practitioners as well as patients. HIPAA was primarily intended to give workers and their families the right to transfer their health care insurance from one job to another without penalties and to simplify administrative processes in transmitting information, especially electronically. HIPAA was included as the final section of the law, although it has come to be its most familiar segment. Inevitably, the legislative process involved compromises and ambiguities and only set out the framework.

The Privacy Rule, finalized in 2003 and revised several times since then, was intended to sort out these problems and give providers clear direction. In 2009, as part of the American Recovery and Reinvestment Act (ARRA), the expansion of health information technology was included as the Health Information Technology for Clinical and Economic Health Act (HITECH). This act significantly increased the enforcement provisions of HIPAA, especially around security and transfer of electronic PHI.3

Basically, HIPAA requires “covered entities” (health care providers, health plans, physician practices, pharmacies, and their business partners) to ensure that there are safeguards to protect the security of PHI they gather in the course of doing business. Covered entities and their employees are allowed to disclose this information only to those who have a legitimate need to know to care for the patient or to pay for care.

The “HIPAA Scare” and Enforcement
So far, so good. In many institutions, however, HIPAA was introduced by lawyers and risk managers who stressed the legal and financial consequences of failing to comply with regulations. Regardless of the trainers’ intent, staff members who attended these sessions clearly heard the message, “If you want to be safe, don’t tell anyone anything.” The result was what has been called the “HIPAA scare,” a situation in which even patients were not given information about their condition because of fears that the nurse or doctor would get into trouble. (Patients’ inability to access their own information is the third most common problem reported to the United States Department of Health and Human Services’ Office of Civil Rights, which is HIPAA’s enforcement arm.) That fear has been passed on to new employees who may trust what they learn through informal communication more than what they are told in formal trainings.

At the same time, fears have been reinforced by reports that institutions have been fined and employees censured or fired because of HIPAA violations. The most publicized violations have been failures to protect large amounts of data, not unwarranted disclosures of individual patient information. In February 2011, Massachusetts General Hospital agreed to pay the government $1 million and to revise its security rules after a hospital employee left the records of 192 patients with infectious diseases, including HIV/AIDS, on a subway car. In March 2012, BlueCross BlueShield of Tennessee agreed to pay $1.5 million for violations under the HITECH breach notification rule after 57 hard drives containing the medical records of a million patients were stolen from a leased facility. After a year-long examination of cybersecurity and vulnerability to hackers, the Washington Post concluded that health care is among the most vulnerable industries in the country, in part because of aging technology and failures to fix known software flaws.4

Some HIPAA violations have involved outright theft—stealing medical records not for the clinical data, but for access to Social Security or credit card numbers or other financial information. Such examples were illegal before HIPAA and are prosecuted by local authorities. Some violations have occurred when staff members not assigned to a particular patient looked at the medical record because of some personal relationship—an ex-spouse or
Of the more than 76,000 HIPAA complaints the Office of Civil Rights has received since April 2003, 91% have been resolved, 18,000 of them through requiring changes in privacy practices and other corrective actions, mostly system changes that affect all patients.

a nasty neighbor, for example.

According to the Department of Health & Human Services’ Office of Civil Rights, as of November 30, 2012, the most frequent sites where instances of noncompliance have been investigated are private practices, general hospitals, outpatient facilities, health plans, and pharmacies. Of the more than 76,000 HIPAA complaints the Office of Civil Rights has received since April 2003, 91% have been resolved, 18,000 of them through requiring changes in privacy practices and other corrective actions, mostly system changes that affect all patients.8

Fears that an individual doctor or nurse can be sued for disclosing information are common but exaggerated. An individual who believes that protected health information has been inappropriately disclosed has no legal recourse under HIPAA other than a complaint to the Office of Civil Rights. Although HIPAA creates a right to privacy, there is no right to sue a doctor, nurse, or hospital. The individual can file a lawsuit under state law alleging violation of privacy, and would bear the burden of proving harm, but HIPAA would not be a factor. State investigations can, however, result in fines. In a California case, a woman discussed with a reporter what she believed to be fraudulent claims to Medicare for a condition she did not have (kwashiorkor, a condition found primarily in malnourished children in poor countries). To defend their claims, hospital executives took her medical record to a local newspaper without her authorization.7 The state fined the hospital $100,000 and ordered the offending executives to consult with its privacy officer before any disclosures.8

With increasing attention under HITECH to breaches of confidentiality and increased penalties, it is possible that a new “HITECH scare” may emerge. While there is ample reason for concern about lax security, it would be unfortunate if this new wave of compliance anxiety overshadowed basic principles of communication and good clinical care.

HIPAA’S Chilling Effect on Communication

Health care currently focuses on encouraging patients and families to become more “engaged,” “activated,” “self-reliant” in care. These efforts, as well as HIPAA itself, assume an adult patient in complete control of decision-making, not an elderly patient who is confused or demented. But many of the patients most at risk for poor outcomes and hospital readmissions—older adults with multiple chronic conditions, including cognitive deficits—are not able to become actively engaged. They rely on a family member or friend to help them at home and to manage or provide follow-up care. Family caregivers—defined as individuals who are responsible for providing or managing care for a chronically ill or disabled person—provide more than 80 percent of long-term care in the community. They are essential to the well-being of patients once they leave the hospital or other facility. They manage doctor appointments, transportation, supplies, and other necessities. In effect, they are care managers without portfolio.

Increasingly they are also expected to perform many complex tasks, such as managing multiple medications, doing wound care, and operating and monitoring equipment. A national survey conducted by the United Hospital Fund and the AARP Public Policy Institute found that nearly half of the family caregivers performed one or more “medical/nursing” tasks, in addition to personal care or household chores.9 Yet 61% of those who found medication management hard said that they learned on their own.

Without family involvement, these patients are likely to return to the Emergency Department and be readmitted, often with the first few weeks after discharge. For patients with heart attack, heart failure, and pneumonia, these readmissions within 30 days can cost the hospital a financial penalty. But when family members ask questions on behalf of the patient and themselves, they are all too often told, “I can’t tell you because of HIPAA.”

HIPAA is not the only reason for the lack of training, of course, but it is part of the general climate that protects staff from real or imagined problems by closing off communication with family caregivers. The task of communicating difficult or time-consuming information is handed off to the next provider, or questions go unanswered until a problem arises. For family caregivers HIPAA fits into the unhappy category of a Law of Unintended Consequences.

What HIPAA Really Says About Sharing Information With Family

As interpreted by the Office of Civil Rights, “HIPAA does not cut off all communications between
providers and the families and friends of patients’ health records with family members and other nonprofessionals. Social support is clearly an important element in managing chronic illnesses, and it is difficult for family and friends intimately involved with the patient’s care to provide that support without relevant information.

Case managers and other health care providers can certainly recall cases in which a patient adamantly refused to have information shared with some or all family members. The reasons may be varied. For example, a relative long out of the family picture shows up unexpectedly and demands information on the patient’s condition. Or the patient has had a long history of disension with a particular family member and does not want to share any information. Often, however, the reason is not related to privacy at all but to a desire not to burden a family member with information and responsibilities. These cases require negotiation, especially if the family member is going to be responsible for follow-up care. At the same time health care providers should not agree to withhold vital information from the patient at the family’s request unless the patient has asked not to be informed. Establishing rules for communication are important and are best accomplished at the outset of care.

Part of the reason HIPAA has been so misunderstood and misused is that it fits neatly into an already well established pattern of keeping family caregivers at arm’s length. From the viewpoint of many providers, families cause trouble. They are emotional and not “objective.” A law that limits sharing information offers a convenient but misguided rationale.

**Recommendations**

Care managers may feel that they are the final link in a chain that they have not designed. While they are often left to piece together the fragments of a care plan that others have only sketched out, they are far from powerless. Here are some recommendations for collective and individual action:

- Convene a group of senior leaders and staff to review relevant elements of the organization’s privacy policies and practices. This should include general information about HIPAA compliance but also any specific practices that deviate from the general rules (requiring written consent, for example, for disclosures to family members). It should also include information about the protections in place to protect the security of data collected and stored in an electronic health record.
- If this discussion reveals concerns or contradictions, suggest establishing a task force to come up with suggestions based on the organization’s mission and practice.
- Encourage staff training (or retraining) on HIPAA and HITECH so that all staff understand the same principles and rules.
- Suggest that the organization create a simple statement of the organization’s policy and practices that patients and family can understand. Patients are required to sign a legal disclaimer that they have been informed about the organization’s policies, but they are usually written in language that only health care lawyers can understand. This simple statement can be useful in discussions with patients and families who are confused about who is being told what and why.
• When dealing with individual patients and families, initiate a discussion about privacy and confidentiality so that they understand the rules. If they have encountered difficulties obtaining relevant information, speak with the staff person responsible and ask for the reasons information was withheld (or was given but not understood).
• In cases that present unusual or challenging issues, discuss them with the organization’s privacy officer before taking any action. Raising potentially serious problems is an important step in reducing HIPAA violations and can protect the institution as well as patients and staff.

REFERENCES


