Protecting privacy

HIPAA's Privacy Rule safeguards personal medical information while allowing research to continue.

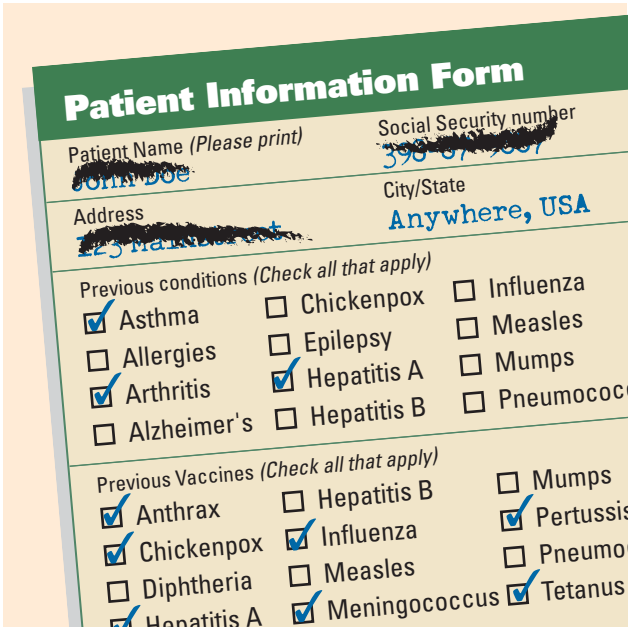
BY CULLEN T. VOGELSON

Ring, ring.
"Hello?"
"Hello, Mr. Smith?"
"Yes, may I help you?"
"Well, actually, I'd like to talk to you about the prescription medication you've been using since last June to treat your worsening case of paranoid schizophrenia. My name is Frank Jones, and I was just reviewing your medical records and thought you might want to know about a new treatment that could help with your condition with fewer side effects. . . ."

In all likelihood, a phone call like this would not calm Mr. Smith's paranoia. But it is not altogether atypical of the kinds of calls, letters, and targeted mass mailings that individuals have increasingly received in past years, partly as a result of the well-publicized disclosure of medical information from pharmacies to marketers. However, in April, a key component of the U.S. government's Health Insurance Portability and Accountability Act of 1996 (HIPAA) took effect that mandates privacy protections for patient health information. The new Privacy Rule affects not only how doctors, hospitals, pharmacists, and insurance companies conduct their businesses, but also how some pharmaceutical manufacturers market their products and how researchers collect, analyze, and report data obtained from human subjects.

Privacy protections

The issues related to privacy are enumerated in the administrative portions of the Act, which contain directives that mandate controls over security, privacy, and so-called electronic data interchanges (e.g., enrollment logs used to track patient participation in research studies and code sets used for insurance billing purposes). The Privacy Rule's principal concern surrounds the use and disclosure of health care information that is directly associated with a particular individual. Specifically, under the Rule, "protected health information" (PHI) can be used without restriction for purposes of payment, treatment, and general "health care operations", and it also may be disclosed for any specified purpose (such as research), provided that patient authorization is obtained first. Failure to comply with the Rule carries civil and criminal penalties of up to $250,000 in fines and 10 years in prison.



In terms of what PHI can be used and disclosed without authorization, it is important to understand that the term "payment" is not limited to simple billing but actually encompasses all activities that health plans undertake (e.g., determining plan eligibility, obtaining premiums, providing member coverage, verifying billing claims, and generating reimbursements). Similarly, the term "treatment" involves more than just the activities that occur between a patient and his or her physician; it also includes activities such as obtaining lab tests from external providers, conducting consultations with other providers, and referring patients to specialists and others. Finally, the phrase "health care operations" refers to all activities that occur between and among designated health and medical organizations (e.g., peer review, student training, quality assurance, premium underwriting, legal services, and cost management).

Thus far, little has been said about what specific, personal information is protected by the Rule, but information that is individually identifiable is safeguarded. This includes demographic information collected from an individual; data created by the process of payment, treatment, or other health care operations; and information about the health and physical well-being of an individual. Furthermore, PHI is held private when it is stored, maintained, or transmitted through either physical or electronic means. The Rule even explicitly lists particular identifiers that may be included in health information that can be used to precisely identify an individual. These identifiers include patient name, address, age (if over 89), birth date, names of relatives and employers, and social security number.

In addition to the above specifications, the Rule identifies three groups, known as "covered entities", which are required to safeguard PHI:

- providers—defined as individuals or organizations that provide health care or medical services and who either bill or are paid for their services (e.g., physicians, nurses, hospitals, and pharmacies),

- health plans—defined as individuals or organizations that pay the cost of health or medical care, and
- clearinghouses—defined as organizations that translate or edit electronic transactions.

Research implications

According to the "common rule" as defined by the *Code of Federal Regulations*, 45 *CFR* 164.501, research is "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." With this in mind, the Privacy Rule was designed explicitly to protect individually identifiable information while simultaneously allowing researchers access to vital medical and health care data.

The privacy of research subjects is guaranteed by the Rule: To use and disclose their PHI, research investigators must obtain authorizations from study participants before entering them in clinical trials. However, not all medical research necessarily requires the disclosure of PHI, and thus, authorizations are not always mandated. For example, data that "de-identifies" patients—in essence, data stripped of individual identifiers—can be used and disclosed without patient authorization. This kind of data may be useful for conducting analyses of health trends and other similar research, but generally it is insufficient for use in supporting research intended to demonstrate the efficacy and safety of novel treatments, pharmaceutical and nonpharmaceutical products, and medical devices.

If an authorization is required, there are several ways in which patient permission may be obtained. In all cases, though, the content of each authorization must clearly describe to patients the scope of the authorization, the manner in which PHI will be used, and to whom it will be disclosed. The Rule specifies that providers may not refuse care to patients who do not grant use-and-disclosure authorizations. In clinical trials, however, since disclosure of certain PHI is vital to the research process, the Rule contains an exception wherein physicians may exclude patients from research studies if they refuse to provide appropriate privacy authorizations.

Obtaining authorization

There are three methods of gaining authorization to use and disclose PHI beyond the unrestricted areas of payment, treatment, and health care operations. These include instituting limited-data-use agreements, receiving use-and-disclosure authorizations from patients, or creating business associate agreements. The last of these methods involves having the covered entity enter into a contractual agreement that effectively passes the privacy obligations on to an unrelated party for the purposes of conducting a limited, specified service (such as quality assurance auditing). This type of agreement, however, generally is not pertinent to research.

A limited-use agreement allows a covered entity to use and disclose a "limited data set" for explicit limited purposes without a patient's approval. In this case, the phrase "limited data set" refers to data that has been largely de-identified. Further, the "limited purposes" requirement narrowly defines the permissible uses of the disclosed information. In general, though, because the restrictions inherent in these types of agreements are significant, their applicability to research is minor.

Data that "de-identifies" patients can be used and disclosed without patient authorization.

By far, the most common form of agreement used in clinical research involves a use-and-disclosure authorization that patients sign prior to the start of a clinical trial. This PHI authorization is distinctly different from the required consent-to-participate document (informed consent) that patients review and sign before enrolling in a trial. The content of the use-and-disclosure authorization is described in 45 *CFR* 164.508. Of particular interest to researchers are three provisions: the authorization, when obtained solely for research purposes, does not have to expire; it may be incorporated either as a component of, or as an addendum to, an informed-consent document; and, as stated previously, the patient's participation in the research project may be conditioned on the patient's willingness to grant a privacy authorization. In all cases, patients have the right to revoke their authorization at any time. For researchers, this final point means that no new PHI may be used or disclosed after an authorization is revoked. To safeguard the integrity of the research process, however, data that has been obtained up to the time of revocation may continue to be used and disclosed in accordance with the originally granted authorization.

Pharmaceutical companies are not covered entities as defined by the Privacy Rule, and thus they are not responsible for obtaining the patient authorizations or for ensuring that they are obtained. However, Investigational Review Boards (IRBs), which are charged with protecting patient safety, are assigned certain responsibilities under the Rule. Specifically, IRBs must ensure that patient privacy protections are adequate in every trial, and they are allowed, when determined to be appropriate, to grant waivers for omissions of required components in the authorizations. Before granting a waiver, the researcher must demonstrate to the IRB that omissions will not impact overall patient privacy, that the research cannot practicably be conducted without the waiver, and that access to PHI is vital to the conduct of the trial.

The Privacy Rule in HIPAA is intended to protect individual medical and health care information that could be used in numerous unscrupulous ways. The Rule is therefore designed to safeguard patient privacy but also to maintain the flexibility necessary to conduct medical research. As with all such protections, the Privacy Rule is not perfect; for example, there is no restriction that prevents disclosed PHI from being redisclosed by a third party without authorization. But overall, the changes to medical practice mandated by the Rule are expected to be a comfort to patients and research participants throughout the country.

Cullen T. Vogelson is a senior clinical research scientist and freelance writer based in Arlington, TX. Send your comments or questions about this article to mdd@acs.org or the Editorial Office address on page 3. ■