United States General Accounting Office

GAO

Testimony

Before the Committee on Health, Education, Labor and Pensions, U.S. Senate

For Release on Delivery
Expected at 9:30 a.m.
Wednesday, February 24, 1999

MEDICAL RECORDS PRIVACY

Uses and Oversight of Patient Information in Research

Statement of Bernice Steinhardt, Director
Health Services Quality and Public Health Issues
Health, Education, and Human Services Division

GAO/T-HEHS-99-70

Medical Records Privacy: Uses and Oversight of Patient Information in Research

Mr. Chairman and Members of the Committee:

We are pleased to be here today to discuss our report on the privacy of medical records used for health research, which was released today.[1] As you know, the increased use of information technology in the health care system and the number of parties with routine access to personally identifiable medical data have raised concerns about the potential misuse of these data and the adequacy of the current system of protections. At the same time, the availability of these data is important for research that can improve the understanding of diseases and treatments across broad populations.

One of the principal mechanisms for overseeing research is the institutional review board (IRB) system. Under the current Federal Policy for the Protection of Human Subjects—which was adopted in 1991 and is known as the Common Rule—research conducted by academic medical centers, pharmaceutical companies, and other organizations that are supported or regulated by any of 17 federal agencies is subject to review by local boards. The Food and Drug Administration (FDA) has regulations nearly identical for oversight of research conducted for drug or medical device approvals. In general, IRBs are meant to ensure that researchers minimize the risks to human research subjects and obtain subjects' informed consent to participate. When appropriate, IRBs are also supposed to consider whether the research projects under their review will protect the privacy of subjects and inform subjects of the extent to which their data will be kept confidential.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L. 104-191) called for protections for the privacy of medical information. Pursuant to HIPAA, the Secretary of Health and Human Services recommended standards with respect to the privacy of personally identifiable information in September 1997. If federal legislation is not enacted by August 1999, the Secretary must promulgate regulations setting privacy standards within 6 months. As you know, a number of bills addressing privacy standards were introduced in the 105th and 106th Congresses, although none has been enacted. As the Congress continues to consider legislation, one concern is to provide access to medical records for the purposes of research while also offering privacy protections.

[1]Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections Is Limited (GAO/HEHS-99-55, Feb. 24, 1999).

In light of these considerations, we examined issues related to the use of medical records for research. In my remarks today, I will describe to what extent medical information used for research depends on personally identifiable information, research that is and is not subject to current federal oversight requirements, and how IRBs ensure the confidentiality of health information used in research. I will also discuss the safeguards health care organizations have in place to protect the confidentiality of health information used in research. We relied extensively on information we collected from 7 IRBs and 12 organizations that conduct health research, including managed care, pharmacy benefit management, pharmaceutical, biotechnology, and health information organizations and integrated health systems.

In summary, our survey revealed that a considerable amount of health research relies on personally identifiable information. While some of this research is subject to IRB review—either because it is federally supported or regulated research or because the organization voluntarily applies federal rules to all of its research—some of the organizations conduct records-based research that is not reviewed by an IRB. In any case, the process of IRB review does not ensure the confidentiality of medical information used in research—primarily because the provisions of the Common Rule related to confidentiality are limited. Moreover, according to recent studies, the IRB system on the whole is strained. Nevertheless, although external review of their research is limited, most of the organizations in our study told us that they have various security safeguards in place to limit internal and external access to paper and electronic databases, and many say they have taken measures to ensure the anonymity of research and survey subjects.

Background

The growth of information technology and changes in the health care delivery system have led to increased use of personal medical information. Numerous organizations collect, store, transmit, and use medical information on individuals, who may have little or no knowledge of the organizations' accessing their personal health data. Some of these databases are extensive, containing records on millions of individuals. The availability of these large databases has made many types of research possible but has increased the potential for misuse of private medical

information, raising concern over issues related to privacy and confidentiality.[2]

The federal system of protections was developed largely in response to biomedical and behavioral research that caused harm to human subjects. To protect the rights and welfare of human subjects in research, the Common Rule requires organizations conducting federally supported or regulated research to establish and operate IRBs, which are, in turn, responsible for implementing federal requirements for research conducted at or supported by their institutions. IRBs are intended to provide basic protections for people enrolled in federally supported or regulated research. Most of the estimated 3,000 to 5,000 IRBs in the United States are associated with a hospital, university, or other research institution, but IRBs also exist in managed care organizations (MCO), government agencies, and as independent entities employed by the organizations conducting the research. IRBs are made up of both scientists and nonscientists.

Health Information Is Needed for a Variety of Research Purposes

The organizations that we contacted primarily conduct health research to advance biomedical science, understand health care use, evaluate and improve health care practices, and determine patterns of disease. These organizations use health-related information on hundreds of thousands, and in some cases millions, of individuals in conducting their research. The MCOs and integrated health systems[3] in our study use medical records data, which are generated in the course of treating patients, to conduct epidemiological research and health services research, such as outcomes and quality improvement studies.[4] For example, one MCO, in conducting a quality improvement study, determined from its claims database whether patients with vascular disease were receiving appropriate medications and reported the findings to patients' physicians to assist in the treatment of their patients.

[2]Privacy refers to the specific right of an individual to control the collection, use, and disclosure of personal information. Confidentiality, a tool for protecting privacy, mandates specific controls on personal data, limiting access and disclosure. The privacy protections of the Common Rule apply to research on human subjects when the researcher obtains information that is individually identifiable. The Common Rule defines a human subject as a living individual about whom a researcher obtains (1) data through intervention or interaction with the individual or (2) identifiable private information. Information is individually identifiable when the identity of the subject is or may be readily ascertained by the researcher or associated with the information.

[3]Integrated health systems are systems of care that can include hospitals, academic medical centers, and primary care physicians and specialists.

[4]Health services research examines the use, costs, quality, accessibility, delivery, organization, financing, and outcomes of health care services to increase the knowledge and understanding of health services for individuals and populations. It includes outcomes research on the benefits and harms of alternative strategies for preventing, diagnosing, or treating illness.

The pharmaceutical and biotechnology companies that we contacted also conduct health services and epidemiological research; but unlike MCOs and integrated health systems, they rely on data from other organizations for this type of research. One pharmaceutical company's epidemiology department, for example, conducts large-scale studies using data from MCOs and health information organizations to monitor the effectiveness of drugs on certain populations.

For pharmacy benefit management (PBM) firms, which administer prescription drug benefits for health insurance plans, a primary source of data is prescription information derived from prescriptions dispensed by mail or claims received from retail pharmacies. PBMs design and evaluate programs that are intended to improve the quality of care for patients who have specific diseases or risk factors while controlling total health care costs. One PBM in our study, for example, develops disease management programs; these programs depend on the ability to identify individuals with conditions, such as diabetes, that require more intensive treatment management.

The health information organizations that we contacted rely solely on data from other organizations. Typically, they collect medical claims data from their clients or obtain it from publicly available sources, such as Medicare and Medicaid.[5] They may also acquire data through employer contracts that stipulate that all the employers' plans provide complete data to a health information organization. Examples of research projects include studies of the effects of low birth weight on costs of medical care and the effectiveness of alternative drug therapies for schizophrenia.

Officials at the organizations we contacted believe that many of these studies require personally identifiable information to ensure study validity or to simply answer the study question. For longitudinal studies, researchers may need to track patients' care over time and link events that occur during the course of treatment with their outcomes. Researchers may also need to link multiple sources of information, such as electronic databases and patient records, to compile sufficient data to answer the research question. For example, officials at one health information organization stated that without patient names or assigned patient codes, it would not have been possible to complete a number of studies, such as the effects of length-of-hospital stay on maternal and child health following delivery and patient care costs of cancer clinical trials.

[5]Clients of health information organizations may include health care providers, health plans and plan administrators, employers, and government health programs.

Federal Requirements Do Not Apply to All Research, but Some Organizations Voluntarily Apply Those Requirements to All Studies

Some of the research conducted by the organizations we contacted must conform to the Common Rule or FDA regulations because it is either supported or regulated by the federal government. Several MCOs obtain grants from various federal agencies, including the Centers for Disease Control and Prevention; one health information organization that we contacted conducts research for federal clients, such as the Agency for Health Care Policy and Research. Some organizations that conduct both federally supported or regulated research and other types of privately funded research choose to apply the requirements uniformly to all studies involving human subjects, regardless of the source of funding.

However, some other organizations that carry out both publicly and privately funded research apply the federal rules where required, often relying on IRB review at collaborators' institutions, but do not apply the rules to their privately funded research. Pharmaceutical and biotechnology companies, for example, rely on the academic medical centers where they sponsor research to have in place procedures for informed consent and IRB review,[6] but they do not maintain their own IRBs.

Some organizations conduct certain activities that involve identifiable medical information, but they do not define these activities as research. For example, officials at several MCOs told us that they did not define records-based quality improvement activities as research, so these projects are not submitted for IRB review. But there is disagreement as to how to classify quality improvement reviews, and some organizations do submit these studies for IRB review, where they define the studies as research.

Finally, at some organizations, none of the research is covered by the Common Rule or FDA regulations and no research receives IRB review. For example, one PBM in our study, which conducts research for other companies—including developing disease management programs—does not receive federal support and, thus, is not subject to the Common Rule in any of its research. While it does not have an IRB, this PBM uses external advisory boards to review its research proposals. Another type of research that for some companies does not fall under the Common Rule or FDA regulations is research that uses disease or population-related registry data. Pharmaceutical and biotechnology companies maintain such registries to monitor how a particular population responds to drugs and to better understand certain diseases.

[6]Pharmaceutical and biotechnology companies that conduct clinical research in-house for FDA regulated products are required to have IRB review and informed consent for that research.

IRB Reviews Provide Limited Oversight of Confidentiality

While many organizations have in place IRB review procedures, recent studies that pointed to weaknesses in the IRB system, as well as the provisions of the Common Rule itself, suggest that IRB reviews do not ensure the confidentiality of medical information used in research. While not focusing specifically on confidentiality, previous studies by GAO and by the Department of Health and Human Services (HHS) Office of Inspector General have found multiple factors that weaken institutional and federal human subjects protection efforts.[7] In 1996, we found that IRBs faced a number of pressures that made oversight of research difficult, including the heavy workloads of and competing professional demands on members who are not paid for their IRB services. Similarly, the Inspector General found IRBs unable to cope with major changes in the research environment, concluding that they review too many studies too quickly and with too little expertise, and recommended a number of actions to improve the flexibility, accountability, training, and resources of IRBs.

Federal Regulations Contain Limited Provisions for Overseeing Confidentiality

Under the Common Rule, IRBs are directed to approve research only after they have determined that (1) there are provisions to protect the privacy of subjects and maintain the confidentiality of data, when appropriate, and (2) research subjects are adequately informed of the extent to which their data will be kept confidential. However, according to the Director of the Office for Protection From Research Risks (OPRR),[8] confidentiality protection is not a major thrust of the Common Rule and IRBs tend to give it less attention than other research risks because they have the flexibility to decide when it is appropriate to review confidentiality protection issues.

Consistent with federal regulations, the seven IRBs that we contacted told us that they generally waive the informed consent requirements in cases involving medical records-based research.[9] Researchers at the organizations we visited contend that it is often difficult, if not impossible, to obtain the permission of every subject whose medical records are used.

[7]Scientific Research: Continued Vigilance Critical to Protecting Human Subjects (GAO/HEHS-96-72, Mar. 8, 1996) and HHS Office of Inspector General, "Institutional Review Boards: A Time for Reform," OEI-01-97-00193 (June 1998).

[8]OPRR is within the National Institutes of Health (NIH) and is the oversight agency for HHS-supported research.

[9]A waiver or modification of informed consent may be permitted if an IRB finds and documents that: the research involves no more than minimal risk; the rights and welfare of subjects will not be adversely affected; the research could not practicably be carried out without the waiver or alteration of the consent requirement; and, whenever appropriate, subjects will be provided with pertinent information after participation. FDA regulations do not permit a waiver of consent.

As an example, the director of research at one integrated health system described a study that tracked about 30,000 patients over several years to determine hospitalization rates for asthmatic patients treated with inhaled steroids.

The IRBs that we contacted told us that they routinely examine all research plans using individually identifiable medical information to determine whether the research is exempt from further review, can receive an expedited review,[10] or requires a full review. Further, in reviewing research using individually identifiable genetic data, two of the IRBs had policies to consider additional confidentiality provisions in approving such research.

Some Breaches of Privacy Have Been Reported

The actual number of instances in which patient privacy is breached is not fully known. While there are few documented cases of privacy breaches, other reports provide evidence that such problems occur. For example, in an NIH-sponsored study, IRB chairs reported that lack of privacy and lack of confidentiality were among the most common complaints made by research subjects.[11] Over the past 8 years, OPRR's compliance staff has investigated several allegations involving human subjects protection violations resulting from a breach of confidentiality. In the 10 cases provided to us, complaints related both to research subject to IRB review and to research outside federal protection.[12]

In certain cases involving a breach in confidentiality, OPRR has authority to restrict an institution's authority to conduct research that involves human subjects or to require corrective action. For example, in one investigation, a university inadvertently released the names of participants who tested HIV positive to parties outside the research project, including a local television station. In this case, OPRR required the university to take corrective measures to ensure appropriate confidentiality protections for human subjects. In response, the university revised internal systems to prevent the release of private information in the future.

[10]An expedited review may be conducted by the chairperson or a chair-appointed IRB member rather than the full board.

[11]James Bell Associates, "Final Report: Evaluation of NIH Implementation of Section 491 of the Public Health Service Act, Mandating a Program of Protection for Research Subjects," prepared for NIH's Office of Extramural Research (June 1998).

[12]Additional cases may have been reported to OPRR, but these were examples the staff could readily identify that involved breaches of confidentiality.

However, in other cases, OPRR determined that it could not take action because the research was not subject to the Common Rule and, thus, it lacked jurisdiction. For example, in a case reported in the media, OPRR staff learned of an experiment that plastic surgeons had performed on 21 patients using two different facelift operations—one on each half of the face—to see which came out better. OPRR staff learned that the study was not approved by an IRB and that the patients' consent forms did not explain the procedures and risks associated with the experiment. In addition, the surgeons published a journal article describing their research that included before and after photographs of the patients. Because the research was performed in physician practices and was not federally supported, it fell outside the Common Rule and OPRR could take no action.

Organizations Conducting Research Have Measures to Reduce Access to Personally Identifiable Information

Each organization that we contacted reported that it has taken one or more steps to limit access to personally identifiable information in their research. Many have limited the number of individuals who are afforded access to personally identifiable information or limited the span of time they are given access to the information, or both. Some have used encrypted or encoded identifiers to enhance the protection of research and survey subjects.[13] Most, but not all, of the organizations have additional management practices to protect medical information, including written policies governing confidentiality. Some organizations have also instituted a number of technical measures and physical safeguards to protect the confidentiality of information.

Officials from two of the companies that we contacted told us that they did not have written policies to share with us, and two other companies were unable to provide us with such documentation, although officials described several practices related to confidentiality. The organizations that did provide us with documentation appear to use similar management practices and technical measures to protect health information used in their health research, whether they generate patient records or receive them from other organizations.

To limit access, several organizations have created special subset databases to enable them to limit researchers' access to information that is

[13]Data are considered "encoded" or "encrypted" when personal identifiers and means of directly contacting an individual (for example, name, address, and social security number) are replaced with numeric or other coding. "Anonymized" data are those from which all personal identifiers have been removed or information aggregated in a manner so that individuals cannot be identified. Medical and health data used by organizations when they conduct health research are viewed as fully identifiable when a name, address, or another identifier is associated with the data.

relevant to their studies. In addition to limiting access to certain individuals for specific purposes, some organizations have encrypted or encoded patient information. Researchers at one integrated health system, for example, work with information that has been encoded by computer programmers on the research team—the only individuals who have access to the fully identifiable data.

In conducting collaborative research, the organizations that we contacted tend to use special data sets and contracting processes to protect medical information. For example, one MCO, which conducts over half of its research with government agencies and academic and research institutions, transfers data in either encrypted or anonymized form and provides detailed specifications in its contracts that limit use of the data to the specific research project and prohibit collaborators from re-identifying or transferring the data.

Generally, company policies define the circumstances under which personally identifiable information may be disclosed and the penalties for unauthorized release of confidential information. Most company policies permit access only to the information that is needed to perform one's job; 8 of the 12 organizations also require their employees to sign agreements stating that they will maintain the privacy of protected health information.

Each organization that we contacted said it uses disciplinary sanctions to address employee violations of confidentiality or failure to protect medical information from accidental or unauthorized access, and an intentional breach of confidentiality could result in employee termination—which may be immediate. But they also pointed out that few employees have been terminated, and when they have, the incidents were not related to the conduct of research.

The organizations that we contacted said they use a number of electronic measures to safeguard their electronic health data. Most reported using individual user authentication or personal passwords to ensure users access only the information that they need; some also use computer systems that maintain an electronic record of each employee who accesses medical data. These organizations may also use other technical information system mechanisms, including firewalls, to prevent external access to computer systems. In addition to electronic security, officials at some of the organizations told us they use various security measures to prevent unauthorized physical access to medical records-based information, including computer workstations and servers.

Conclusions

Personally identifiable information is often an important component of research using medical records, and the companies we met with furnished many examples of useful research that could not have been conducted without it. Because our study focused on only a limited number of companies—in particular, those that were willing to share information about corporate practices—it is difficult to judge the extent to which their policies may be typical, nor do we know the extent to which their policies are followed. Nevertheless, most of the organizations we surveyed do have policies to limit and control access to medical information that identifies individuals, and many of them have adopted techniques, such as encryption and encoding, to further safeguard individual privacy.

However, while reasonable safeguards may be in place in these companies, external oversight of their research is limited. Not all research is subject to outside review, and even in those cases where IRBs are involved, they are not required to give substantial attention to privacy protection. Further, in light of the problems that IRBs have had in meeting current workloads—one of the key findings of our earlier work as well as the work of HHS' Office of Inspector General—it is not clear that the current IRB-based system could accommodate more extensive review responsibilities. In weighing the desirability of additional oversight of medical records-based research, it will be important to take account of existing constraints on the IRB system and the recommendations that have already been made for changes to that system.

This concludes my prepared statement. I will be happy to respond to any questions that you or Members of the Committee may have.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested