United States General Accounting Office

GAO

Report to Congressional Requesters

February 1999

MEDICAL RECORDS PRIVACY

Access Needed for Health Research, but Oversight of Privacy Protections Is Limited

GAO/HEHS-99-55

GAO

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

Health, Education, and
Human Services Division

B-280657

February 24, 1999

The Honorable James M. Jeffords
Chairman, Committee on Health, Education,
Labor, and Pensions
United States Senate

The Honorable Christopher J. Dodd
Ranking Minority Member
Subcommittee on Children and Families
Committee on Health, Education,
Labor and Pensions
United States Senate

Historically, patient medical records were used largely by physicians and medical insurers. However, with the creation of electronic records and large databases of medical information, the number of health care professionals and organizations with access to medical records has increased. While such availability allows for research that can improve the understanding of diseases and treatments across broad populations, the number of parties with routine access to personally identifiable medical data has raised concern about the potential misuse of these data and the adequacy of the current system of protections.

Under the current Federal Policy for the Protection of Human Subjects, adopted in 1991 and known as the Common Rule, research conducted by organizations, such as academic medical centers and pharmaceutical companies, that is supported or regulated by any of 17 federal agencies is subject to certain federal oversight requirements.[1] In accordance with the Common Rule, organizations have established local institutional review boards (IRB), made up of both scientists and nonscientists, to review whether researchers minimize the risks to research subjects and obtain their informed consent. When appropriate, IRBs are also supposed to consider whether the research projects under their review will protect the privacy of subjects and inform them of the extent to which their data will be kept confidential. In addition, pharmaceutical companies and other

[1]Department of Health and Human Services (HHS) regulations—codified at title 45, Part 46, Subpart A of the Code of Federal Regulations—apply to research involving human subjects that is conducted, supported, or regulated by HHS. In addition, the following agencies have adopted regulations incorporating the substance of the HHS regulations: Departments of Agriculture, Commerce, Defense, Education, Energy, Housing and Urban Development, Justice, Transportation, and Veterans Affairs; the Agency for International Development; the Central Intelligence Agency; the Consumer Product Safety Commission; the Environmental Protection Agency; the National Aeronautics and Space Administration; the National Science Foundation; and the Social Security Administration.

manufacturers of certain medical products must also meet Food and Drug Administration (FDA) regulations, which closely resemble the Common Rule, for research they conduct in connection with their FDA-regulated products.[2] Organizations conducting research that is not federally supported or regulated can use IRBs if they choose but are generally not required to do so.

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 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 of HHS must promulgate regulations setting privacy standards within 6 months. Bills related to medical records privacy introduced in the 105th and 106th Congresses have provisions to address uses of medical information for a variety of purposes, including research.[3] The various bills attempt to provide for the conduct of medical research while also offering privacy protections, and some of them call for extending the current requirements of the Common Rule, including the use of IRBs, to research that is not federally supported or regulated. No legislation has been enacted.

However, little is known about the types of health research conducted outside the Common Rule and FDA regulations and what safeguards may already be used for such research. Therefore, you asked us to (1) examine how medical information is used for research and the need for personally identifiable information, (2) identify research that is and is not subject to current federal oversight requirements, (3) examine how IRBs ensure the confidentiality of health information used in research, and (4) identify the safeguards health care organizations have put in place to protect the confidentiality of health information used in research.

To conduct our work, we reviewed health research and privacy literature and interviewed experts in these fields and officials from various health industry associations. We also reviewed HHS documents and met with officials from HHS and, from within the Department, FDA, and the National

[2]FDA regulations are codified at title 21, Parts 50 and 56 of the Code of Federal Regulations.

[3]Bills introduced in the 105th and 106th Congresses to set up standards for the privacy of medical records include S. 2609, 105th Cong. (1998) (introduced by Sen. Bennett); S. 1921, 105th Cong. (1998) (introduced by Sen. Jeffords); S. 1368, 105th Cong. (1997) (introduced by Sen. Leahy); H.R. 1815, 105th Cong. (1997) (introduced by Rep. McDermott); H.R. 52, 105th Cong. (1997) (introduced by Rep. Condit); S. 300, 106th Cong. (1999) (introduced by Sen. Lott); and S. 326, 106th Cong. (1999) (introduced by Sen. Jeffords).

Institutes of Health (NIH). We also interviewed representatives from seven IRBs and officials from two state departments of health. Five of these IRBs were at institutions that conduct research for the federal government, and two are freestanding IRBs that are hired for their services. In addition, we reviewed documents and interviewed officials from 12 organizations that conduct health research not subject to the Common Rule or FDA regulations, including managed care, pharmacy benefit management, pharmaceutical, biotechnology, and health information organizations and integrated health systems. For the most part, organizations provided documentation of their policies on confidentiality and information safeguards; however, we did not assess the implementation of these policies. Given the limited number of organizations in our review, their research and safeguard practices and the practices of the IRBs should not be considered representative of those organizations on the whole. We conducted our work between July 1998 and February 1999 in accordance with generally accepted government auditing standards. A detailed description of our scope and methodology is provided in appendix I.

Results in Brief

Medical information is used for a number of research purposes—to advance biomedical science, understand health care utilization, evaluate and improve health care practices, and determine causes and patterns of disease. While such research is sometimes conducted without information tied to identifiable patient records, other research relies on personal identifiers to track treatment of an individual over time, link multiple sources of patient information, or verify such information.

Some of the research conducted by the organizations we contacted must conform to the Common Rule or FDA regulations because the research is either federally supported or regulated. But many of these same organizations voluntarily apply federal rules, including IRB review, to all their research, regardless of source of funding. Other organizations choose not to apply the Common Rule and IRB review where not required. For example, research conducted by pharmacy benefit management companies, which conduct studies for other companies, is not federally supported or regulated and is, therefore, outside the Common Rule, and they do not use IRB review.

In any case, IRB review does not ensure the confidentiality of medical information used in research because the provisions of the Common Rule related to confidentiality have limitations. Records-based research is often subject to an expedited review process—under which only one board

member, rather than the full IRB, considers the research proposal. In addition, IRBs can waive informed consent requirements, including the requirement to inform people of the extent to which their data will be kept confidential, if they judge that research subjects are not likely to be harmed and that the research could not be carried out without the waiver—as in cases where there are too many subjects to inform. The IRBs we contacted rely on the existence of general organizational confidentiality policies for protecting personal information. While the extent to which IRB practices protect the privacy of research subjects is not fully known, several examples of breaches of confidentiality reported to NIH's Office for Protection From Research Risks (OPRR), the oversight agency for HHS-supported research, illustrate the potential for harm resulting when medical information used in research is not adequately protected.

Although external review of their research is limited, the organizations that we contacted reported they have taken steps to limit access to personally identifiable information. Most of the organizations have various security safeguards to limit internal and external access to paper and electronic databases, and many have taken measures to ensure the anonymity of research and survey subjects. In addition, all but two of the organizations that we contacted have written confidentiality policies restricting employee use and access to health information.

Background

Numerous organizations collect, store, transmit, and use individuals' medical information, which includes data, documents, records, and pathological and diagnostic specimens. These individuals may have little or no knowledge of the organizations' accessing their personal health data. For example, records of patient care—whether through a hospital, private physician, or managed care setting—may be used for health research. The establishment of large computer databases—some with millions of patient records—has not only allowed for such research but has increased the potential for misuse of private medical information, raising concern over issues related to privacy and confidentiality.[4] While IRB reviews may help protect the privacy of subjects and maintain the confidentiality of data

[4]Privacy refers to the specific right of an individual to control the collection, use, and disclosure of personal information. Confidentiality is a tool for protecting privacy. Confidentiality is implemented through specific controls on personal data, limiting access and disclosure. The privacy provisions 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.

used for research, privacy advocates and others argue that any use or disclosure of an individual's medical information should require the individual's informed consent. They view this as important because the failure to adequately safeguard sensitive medical information can affect employment or the ability to receive insurance or lead to other harmful outcomes.

The federal system of protections was developed largely in response to biomedical and behavioral research that caused harm to human subjects. In 1991, many federal agencies standardized their oversight of research involving human subjects with the adoption of the Common Rule. Each institution engaged in research subject to the Common Rule must assure the agency supporting or regulating the research that it follows basic ethical principles underlying the acceptable conduct of research involving human subjects. Currently, 17 federal departments and agencies adhere to the Common Rule.

To protect the rights and welfare of human subjects recruited to participate in research, the Common Rule requires research organizations 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. Among these are an independent review of the risks and benefits of the research. Another protection is informed consent, which requires researchers to inform potential subjects of the risks to which they, as study participants, agree to be exposed. In addition, IRBs have to make sure that, when appropriate, there are adequate provisions in the research plans to protect the privacy of subjects and maintain the confidentiality of data.

Most of the estimated 3,000 to 5,000 IRBs in the United States are associated with a hospital, university, or other research institution; however, IRBs also exist in managed care organizations (MCO), government agencies, and as independent entities employed by the organizations conducting the research. Federal requirements specify that IRBs must have at least five members, including one with primarily scientific interests, one with primarily nonscientific interests, and one otherwise unaffiliated with the institution in which the IRB resides. Each of the 17 federal Common Rule agencies has independent responsibility for oversight of IRBs reviewing the research that it supports. However, two HHS agencies—NIH and FDA—exercise the broadest IRB oversight responsibilities. OPRR, located

within NIH, is responsible for monitoring protection of human subjects within all HHS-supported biomedical and behavioral research. FDA is responsible for protecting the rights of human subjects enrolled in research involving products it regulates—drugs, medical devices, biologics, foods, and cosmetics. If research supported by HHS also involves a product regulated by FDA, both agencies have oversight responsibilities.

Pursuant to HIPAA, the Secretary of HHS submitted to the Congress in September 1997 recommendations on privacy standards that may guide legislation for protecting individually identifiable information and to establish penalties for wrongful disclosure of such information. The Secretary recommended that health care providers and payers be permitted to disclose identifiable patient information, without consent, for research under controlled conditions—including approval by an IRB under conditions essentially the same as the present Common Rule—and that further disclosure be sharply restricted. The Secretary's recommendations would also require researchers who obtain information from providers to establish and maintain appropriate safeguards for protecting the confidentiality and security of personally identifiable health information.

Legislative proposals governing medical records privacy under consideration in the 105th Congress contained provisions resembling the Secretary's recommendation. The bills differed, however, in how protected health information was defined and the extent to which reviews by IRBs or other entities would be required for research using personally identifiable health information. If legislation on privacy standards is not enacted by August 1999, HIPAA provides that the HHS Secretary must promulgate final regulations containing standards for confidentiality by February 2000.

In the absence of comprehensive federal legislation, the federal government and some states have enacted laws to protect the privacy of certain medical information. For example, personal information about subjects of drug abuse research can be protected under the Federal Controlled Substances Act. California law permits disclosure of identifiable health information for research purposes without the patient's consent but expressly prohibits any disclosure by the researcher of information that permits identification of the patient. Minnesota's law allows access to medical record information for research unless patients deny their consent, which must be requested.

Personally Identifiable 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 causes and patterns of disease. Within biomedical research, several of the organizations conduct clinical trials to develop new medical products and devices. All of the organizations conduct studies to improve health care practices, such as studies focusing on the most appropriate care for patients with chronic diseases. In addition, nearly all of the organizations conduct epidemiological research—research on the causes and distribution of diseases.

Organizations that provide and pay for care, such as MCOs, generate original medical data, which they can then use for their research. Other organizations—such as those that provide health information services ranging from software development to targeted health research—rely on data from health care providers and payers, some of which contain personal identifiers. Some of these organizations' studies are carried out without personally identifiable health information, but other research requires that, at some point, individual identifiers be known.

Patient Data to Conduct Research Come From Various Sources

The organizations we contacted use health-related information on hundreds of thousands, and in some cases millions, of individuals in conducting their research. There are primarily three sources of data that organizations rely on. Some organizations use data that they generate in providing health care services, and some rely on data acquired from others; some organizations also use data generated as part of their research.

The MCOs and integrated health systems[5] that we contacted primarily rely on data that are self-generated—through either service delivery or research. They use medical record 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.[6] One MCO cited over 40 outcomes studies it conducted on prevention, disease management, and issues related to the structure of the health care delivery system. Another MCO, in conducting a quality improvement study,

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

[6]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.

used its claims database, along with published treatment guidelines, to determine whether patients with vascular disease were receiving appropriate medications. The MCO then provided each patient's treating physician a report based on this analysis to encourage them to review the case; verify the accuracy of the data; and determine whether, in the physician's judgment, any actions were appropriate, such as arranging return visits for these patients and amending their drug regimens.

The pharmaceutical and biotechnology companies that we contacted rely on data from each of the three sources. To support their applications for new drugs and medical devices, they sponsor clinical trials conducted at MCOs and academic medical centers. These companies 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. For example, one pharmaceutical company's epidemiology department conducts large-scale studies to monitor the effectiveness of treatments in clinical practice and studies to track the effects of drugs on certain populations. These studies rely on data the company obtains from MCOs and health information organizations.

Pharmacy benefit management (PBM) firms, which administer prescription drug benefits for health insurance plans, typically generate their own data and obtain data from other organizations. For the PBMs we contacted, a primary source of data is prescription information derived from prescriptions dispensed by mail or claims received from retail pharmacies. The PBMs also use data from other organizations, such as MCOs, to 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. For example, one PBM develops disease management programs, which 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.[7] They may also acquire data through employer contracts that stipulate that all of the employers' plans provide complete data to a health information organization. Examples of research projects include

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

studies of the effects of low birth weight on costs of medical care and the effectiveness of alternative drug therapies for schizophrenia.

Personally Identifiable Information Is Essential for Some Research

Officials at the organizations we contacted believe that a number of studies require personally identifiable information to ensure study validity or to simply answer the study question. For example, to validate initial selection of individuals meeting diagnostic and other criteria as research subjects, researchers may need to review individual patient records. In the case of a research project involving registry data, researchers first determine the feasibility of a study by identifying the likely number of patients meeting certain criteria.[8] They then review patient records to obtain more specific information and to validate the study cohort.

Officials at the organizations we contacted also indicated that their researchers may need to contact patients or review medical records to validate the quality of data used in their research studies. To prevent error, researchers at one MCO use identifiable data to check for duplicate records or redundant cases. If some item in the analysis appears to show an unusual result for an individual, the researchers may need to check the original file to determine if the information was miscoded. Officials at another MCO described a project that required verifying existing claims data on prenatal visits to evaluate whether women had received prenatal care in the first trimester of pregnancy. To verify the data, researchers telephoned patients to obtain information and subsequently conducted a medical records review. Both the self-reported data and the medical records review showed much higher rates of early prenatal care than the claims data had indicated.

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 we contacted stated that without patient names or assigned patient codes, it would not have been possible to complete a number of studies—including studies of the effects of length-of-hospital stay on maternal and child health following delivery and studies on patient care costs of cancer clinical trials. For longitudinal studies, researchers may need to track patients' care over time and link events that occur

[8]Registries are databases that collect information on the experience of populations or special groups over time and can be used by researchers to investigate disease characteristics, the impact of various treatments, and to answer other research questions. For example, a registry maintained by one company might pool physician-contributed patient data on individuals with a particular disease to learn about the disease's natural history, its expected course, and patient response to treatment.

during the course of treatment with their outcomes. For example, officials at an MCO we contacted used identifiable patient data to link asthma patients' records over time to determine if specialist care for the disease improved patient outcomes and lowered costs.

Health care organizations acknowledge that some types of their research can be accomplished without access to information that is fully identifiable. For example, according to officials at one pharmaceutical company we contacted, the company conducts epidemiological research to understand the kinds of patients that are likely to develop a disease, the effectiveness of existing treatments, the types and rates of complications, and the costs and medical care associated with the disease. They said that much of their research is based on data on unidentified individuals that come from federally sponsored surveys or databases, such as survey data from the National Center for Health Statistics or Medicare data from the Health Care Financing Administration.

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 the research is either supported or regulated by the federal government. Several MCOs that we contacted obtain grants from the Centers for Disease Control and Prevention and other federal agencies, and one health information organization that we contacted conducts research for the Agency for Health Care Policy and Research and similar federal clients. Some of the organizations that we contacted, including the integrated health systems and several MCOs, operate IRBs to comply with federal requirements.

While privately funded research that is not in support of a regulated product is not subject to federal requirements, some organizations that conduct both federally supported or regulated research and privately funded research apply the requirements uniformly to all studies involving human subjects, regardless of the source of funding. Organizations conducting a large number of HHS-supported studies may enter into a multiple project assurance (MPA) that commits them to comply with federal regulations on all their research projects involving human subjects, not just those funded by HHS. Even without an MPA, some organizations have adopted internal policies requiring that all studies that meet their definition of research follow Common Rule requirements. As a result, application of the Common Rule to various types of health services research can vary within and across organizations.

Universities and other major research centers that conduct a substantial number of HHS-supported studies and have demonstrated a willingness and the expertise to comply with human subject protections often apply for MPAs with HHS, which are approved by OPRR. Through an MPA, an organization commits itself to full compliance with informed consent and other federal standards. In addition, an institution with an MPA does not need to apply to OPRR for eligibility to receive HHS funds for each new study approved by its IRB. Two of the organizations we visited—both integrated health systems—have MPAs.

Some organizations that do not have an MPA still adopt a policy requiring IRB review of all projects. Two of the MCOs we contacted voluntarily subjected their research to scrutiny by an IRB. At one, the IRB administrator told us that the MCO's IRB gives non-federally funded research the same scrutiny as federally funded research. The IRB at the other MCO, which was established when the MCO's research center was created, follows federal guidelines for the protection of study participants and reviews all studies conducted by the center.

Other organizations that we contacted that carry out both publicly funded and privately funded research do not commit to an MPA. Rather, they apply the federal rules where required, often relying on IRB review at collaborators' institutions, and do not apply the rules to their privately funded research. For example, one MCO that we contacted has a separate research unit that carries out a variety of health studies—some initiated by the MCO, some funded by other private sources, and some federally funded in collaboration with universities or other research institutions. Since the MCO does not maintain its own IRB, it relies on IRB reviews at collaborators' institutions. Still other organizations, such as pharmaceutical and biotechnology companies, rely on the academic medical centers where they sponsor research to have in place procedures for informed consent and IRB review.[9]

However, even where organizations submit both publicly funded and privately funded research to an IRB, certain activities that involve identifiable medical information may not be included because the organization does not define the project as research. For example, at several MCOs, officials told us that they did not define records-based quality improvement activities as research, so these projects are not submitted for

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

IRB review. Some organizations, however, do submit quality improvement 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, does not receive federal support and, thus, is not subject to the Common Rule in any of its research. Their research includes developing disease management programs. While they do not have an IRB, this PBM uses external advisory boards to review 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.

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. The IRB officials we spoke with told us that, for some research, they waive consent provisions and conduct expedited reviews, as permitted by the Common Rule. Most IRBs that we contacted told us that they rely on the existence of general organizational confidentiality policies to protect information. While the extent to which IRB practices protect the privacy of research subjects is not fully known, several examples of confidentiality breaches reported to OPRR illustrate the harm resulting when medical information used in research is not adequately protected.

Earlier Studies Revealed Weaknesses in the IRB System

In recent years, concern has been raised about the adequacy of the IRB system for overseeing the protection of human subjects. While not focusing specifically on confidentiality, previous studies by GAO and by HHS' Office of Inspector General have found multiple factors that weaken institutional and federal human subjects protection efforts.[10] In 1996, we found that IRBs faced a number of pressures that made oversight of research difficult, including the heavy workloads of and competing

[10]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). With the HHS report, there are three companion reports, entitled "IRBs: Their Role in Reviewing Approved Research," "IRBs: Promising Approaches," and "IRBs: The Emergence of Independent Boards."

professional demands on members who are not paid for their IRB services. We also concluded that the effectiveness of human subjects protections can be weakened by the complexity and volume of research under review and the difficulty of ensuring that individuals understand the risks they may experience as research subjects.

Similarly, a 1998 HHS Office of Inspector General report 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. HHS' Inspector General also concluded that IRBs conduct only minimal oversight of approved studies, face conflicts of interest that threaten their independence, and provide little training for investigators and board members. The Inspector General noted that neither IRBs nor HHS staff devote much attention to evaluating IRB effectiveness and made recommendations for changes to improve the flexibility, accountability, training, and resources of IRBs.

Federal Regulations Contain Limited Provisions for Overseeing Confidentiality

The Common Rule, which was developed largely to protect the rights and safety of human subjects, contains two general provisions to protect the privacy of human subjects and the confidentiality of data that identify research subjects.[11] Specifically, 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) as one of the elements of informed consent, research subjects are adequately informed of the extent to which their data will be kept confidential. According to the Director of OPRR, confidentiality protections are 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.

In addition, the Common Rule assumes that the risks presented by some research are sufficiently low that more limited types of review of privacy protection will be adequate. According to the Common Rule, research with medical information can be exempted from review by IRBs and from requirements for prior informed consent when (1) the data are existing at the time the research is proposed and (2) either the sources are publicly available or information is recorded by the investigator in such a manner that subjects cannot be identified—directly or through identifiers linked to

[11]HHS or FDA may also award a Certificate of Confidentiality for a research project, which provides immunity from compelled disclosure, such as subpoenas seeking the identities of subjects enrolled in the study.

the subjects. Alternatively, research involving medical records that presents no more than minimal risk of harm to subjects may be reviewed by the IRB under expedited procedures, even when the data are personally identifiable. Under expedited procedures, the review may be carried out by the chairperson or a chair-appointed IRB member, rather than the full board.

Further, research using individually identifiable information may be permitted by an IRB with a waiver or modification of informed consent if the IRB finds and documents that each of the following criteria has been satisfied:

(1) the research involves no more than minimal risk to subjects (that is, no greater harm than ordinarily encountered in daily life);

(2) the rights and welfare of subjects will not be adversely affected;

(3) the research could not practicably be carried out without the waiver or alteration of the consent requirement; and

(4) whenever appropriate, subjects will be provided with pertinent information after participation.[12]

IRBs Follow Common Rule Criteria for Waiving Consent Requirements and Providing Expedited Reviews for Some Research

Consistent with federal regulations, the seven IRBs that we contacted told us that they generally waive informed consent requirements in cases involving medical records-based research. For research using individually identifiable medical information that does not involve direct contact with patients, IRBs often conduct an expedited review and usually do not require researchers to obtain specific authorization from patients before using their medical records for research.

Under the Common Rule, the IRB may waive consent requirements if the research meets the four criteria above, including that it cannot practicably be carried out without the waiver or alteration of the requirements. If the IRB waives consent requirements, medical records may be available for research without the knowledge or consent of the subjects, even when they are individually identifiable. For some studies, especially epidemiological studies, researchers need to review thousands of records to identify appropriate subjects for their study. Researchers at the

[12]Regulations governing clinical research conducted on FDA regulated products involving no greater than minimal risk do not permit a waiver of consent.

organizations we visited contend that it is often difficult, if not impossible, to obtain the permission of every subject whose medical records are contained in the files. 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. He stated that it would have been impossible to obtain the informed consent of every patient because treatment was provided over a long period of time. Obtaining consent from the patients whose records were used would have been time consuming and expensive, he said, and some patients would have died or would no longer be members.

The Common Rule also permits IRBs to use expedited review procedures—which involve review by only the chairperson or a chair-appointed IRB member, rather than the full board—if the research presents no more than minimal risk of harm to subjects, even when the medical record data used in the research are personally identifiable. A recent NIH-sponsored study found that 58 percent of IRBs affiliated with major research institutions with multiple project assurances performed an expedited review of research using individually identifiable information.[13] The study concluded that the IRBs' standard practice was to use expedited procedures to review research that involves minimal risk.

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, 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.

Several IRBs that we interviewed have some special requirements to ensure that researchers had adequate provisions to protect the confidentiality of individually identifiable information. To obtain IRB approval of research using individually identifiable medical information, three organizations required their researchers to complete applications that included detailed discussions of provisions to protect the privacy of subjects and to maintain the confidentiality of data. The applications typically address who will access research information and how confidentiality of records will be maintained. In another study requiring analysis of personal data on health plan members, the IRB required that everyone involved in conducting the study sign strict confidentiality agreements.

[13]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).

IRBs Rely on Organizational Policies to Ensure Confidentiality

The IRBs in our study told us that they rely on organizational policies to ensure the confidentiality of information used in projects using personally identifiable medical information. For example, the IRB chair and administrator at one integrated health system told us that they rely on the general expectation that all employees will safeguard information about patient medical records. They viewed this as part of the culture of the organization and saw it as a primary mechanism for protecting patient privacy.

Organizational policies to protect information may include restricting access to personally identifiable information to authorized individuals. For example, two integrated health systems we met with require that researchers have an IRB project number, indicating approval to access individually identifiable data. Organizations may also have data security safeguards and policies for imposing sanctions for unauthorized access to or dissemination of personally identifiable medical information.

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 complaints about the lack of privacy and confidentiality were among the most common complaints made by research subjects. Over the past 8 years, OPRR's compliance staff have investigated several allegations involving human subject 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.[14]

In certain cases involving a breach in confidentiality, OPRR has authority, for example, 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 multiple study participants testing positive for HIV to parties outside the research project, including a local television station. In this case, OPRR worked with the university to evaluate the extent of the breach of confidentiality and form a plan to discuss the events with study subjects. In response, the university revised internal systems to prevent the release of private information in the future.

[14]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 one reported case, OPRR learned that during a research presentation at a national meeting, notes on a patient suffering from extreme depression and suicidal impulses stemming from a history of childhood sexual abuse were distributed. The notes included the patient's identity, medical history, mental status and diagnosis, as well as extensive intimate details about the patient's experience. In another case, which was reported in the media, OPRR 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 physicians did not give the patients consent forms explaining in detail 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 its 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.[15] 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.

While each organization has taken one or more of these measures, not all have written policies. 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

[15]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 is viewed as fully identifiable when a name, address, or another identifier is associated with the data.

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. Officials at one integrated health system that we contacted told us that they have an institutional policy on confidentiality of health information, an institutional policy directing access to and security of medical records information, and a human resources policy for maintaining the confidentiality and privacy of personally identifiable patient data.

Special Databases and Encrypted Data Help Organizations Limit Access to Patient Data

To limit access, several organizations have created special subset databases to enable them to limit researchers' access to information that is relevant to their studies. For example, researchers at one MCO conduct studies using a special research database that links hospital, physician visit, and pharmacy claims data for each enrollee and includes information on procedures, diagnoses, and costs of care. Typically, data—with each patient's identity encoded—are extracted from this database for analysis. The researchers do not have routine access to the MCO's larger, fully identifiable claims database.

In addition to limiting access to certain individuals for specific purposes, some organizations have encrypted or encoded patient information. For example, researchers at one integrated health system that we contacted do not see fully identifiable information. Rather, they 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. The pharmaceutical companies that we contacted also limit access to and encode personally identifiable health information used in research. For example, the clinical trials data that they receive typically do not include the identities of the patients enrolled. Instead, the pharmaceutical companies receive data files with identities encoded, and the identifiable data are retained at the research site. Only designated company officials can access the identifiable information during site visits and only for purposes of monitoring the progress of a clinical trial.

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. The contracts specify that collaborators are not permitted to reidentify or transfer the data. Another MCO that we contacted uses multiple measures to ensure confidentiality of its medical data. In addition to requiring collaborators to follow the same confidentiality requirements as the MCO, they can only access medical data through an MCO researcher assigned to the project. Most of the data are aggregated, but any patient-specific data that are provided are encrypted and the coding methodology remains in-house. In addition, research data provided on a computer disk and mailed are tracked to verify delivery.

At another MCO, the lead investigators annually review a list of the names of the individuals who have access to each research project to ensure that the list is current, which is acknowledged by the investigators' signatures. Similarly, one of the integrated health systems that we contacted requires researchers from outside the organization to seek collaborative relationships with internal researchers and obtain approval for an adjunct appointment. The adjunct researchers would then become subject to the organization's policies and controls.

Management Practices Establish Parameters for Protections

Most of the organizations we contacted have established confidentiality policies delineating who can have access to what information, and most provide employee education and training programs on these policies. Most also have established monitoring practices and sanctions for breaches of confidentiality. Some organizations also used employee agreements and their contract processes to ensure confidentiality.

Ten of the 12 organizations that we contacted had written confidentiality policies that limit and control access to personally identifiable information, although 2 of the 10 did not provide us with documentation of their policies. The policies define the circumstances under which such 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; some dictate that such information should be shared with other employees only on a need-to-know basis. Some organizations provide training to ensure employees understand the confidentiality policy in effect. One MCO's training sessions teach employees to keep records in locked file cabinets, shut down computers when not in use, and not share data with associates. Eight of the 12 organizations that we contacted also require their employees to sign agreements—typically upon hiring and annually

thereafter—stating that they will maintain the privacy of protected health information.

To ensure adherence to confidentiality policies, the organizations reportedly have established various monitoring and disciplinary mechanisms. One MCO told us it reviews a sample of all active research projects and conducts reviews of research study files. In addition to periodic reviews of local area network files, the MCO said it also conducts quarterly inspections of its databases. The MCO's parent organization reportedly conducts internal audits to determine compliance with approved protocols and reviews third-party vendor contracts and system security controls. 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. Generally, officials at organizations that we contacted said that 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. According to officials at one health information organization, the company's overriding principle regarding health information is that each employee is responsible for keeping patient data confidential consistent with the organization's policies and prescribed practices.

Companies Report Use of Electronic and Physical Safeguards

The organizations that we contacted said they use a number of electronic measures to safeguard their electronic health data. Most reported using individual user authentications or personal passwords—controls that ensure users access only the information that they need. These organizations may also use encryption or coding technologies to mask personally identifiable data and other technical information system mechanisms, including firewalls, to prevent external access to computer systems. Officials at one MCO we visited said that their computer system maintains an electronic record of each employee that accesses medical data. The MCO periodically reviews the records to determine if use was appropriate.

In addition to electronic security, officials at some of the organizations we contacted told us they use various security measures to prevent unauthorized physical access to medical record-based information, including computer workstations and servers. For example, officials at one MCO told us that protections for paper records include storing the

information in locked offices and file cabinets and shredding paper-based information when it is no longer needed.

Conclusions

Personally identifiable information is often an important component of research using medical records, and the companies we met with provided 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—a key finding in our earlier work as well as in work conducted by 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.

Agency and Other Reviewer Comments

We obtained technical comments from officials at several HHS agencies with significant research responsibilities—FDA, the Centers for Disease Control and Prevention, the Agency for Health Care Policy and Research, and NIH, including its OPRR—and HHS' Privacy Advocate. We also obtained comments from two outside reviewers with expertise in medical research and privacy issues. A number of the HHS program officials provided additional or corrective information on the provisions of the Common Rule and aspects of research, which we incorporated in the report. Our other expert reviewers found the report to be, on the whole, helpful in the current debate on privacy and research. One of these reviewers, however, questioned our conclusion about how well the IRB system protects privacy, arguing that the evidence pointed out that the system is working well. Our

second reviewer, on the other hand, agreed that the IRB system is already heavily burdened. In response to their concerns and views, we made some changes where we believed it was appropriate to do so, but we continue to believe that the IRB system has limitations that need to be highlighted as policymakers consider expanding its responsibilities.

We are sending copies of this report to the Secretary of HHS and other interested parties. We will also make copies available to others upon request. If you have any questions or would like additional information, please call one of the major contributors listed in appendix II.

Sincerely yours,

Bernice Steinhardt
Director, Health Services Quality
and Public Health Issues

Contents

Letter 1

Appendix I Scope and Methodology 26

Appendix II Major Contributors to This Report 28

Abbreviations

FDA	Food and Drug Administration
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IRB	institutional review board
MCO	managed care organization
MPA	multiple project assurance
NIH	National Institutes of Health
OPRR	Office for Protection From Research Risks
PBM	pharmacy benefit management

Scope and Methodology

To help us understand the nature of research that uses medical records and the types of oversight and safeguards that might be used, we identified and reviewed literature on the use of medical information in health research and met with individuals and representatives from associations and organizations knowledgeable about issues surrounding the use of medical information in health research. We also met with officials and reviewed documents from NIH, the Office for Protection From Research Risks, FDA, and the National Bioethics Advisory Commission. Additionally, we met with HHS' Privacy Advocate. We also met with officials of two state departments of public health.

For this work, we used the Common Rule's definition of research: "a systematic investigation . . . designed to develop or contribute to generalizable knowledge." After we determined that there is no inventory of health research conducted outside Common Rule requirements, with the exception of an informal categorical listing developed by OPRR, we focused our examination on health care organizations conducting research with extensive databases. We chose such organizations because of the potential risk to large numbers of individuals if medical information is not adequately safeguarded. Twelve organizations that conduct health research participated in our review, including managed care organizations, integrated health systems, pharmaceutical companies, health information organizations, pharmacy benefit management companies, and biotechnology companies.

We also screened indemnity insurers, utilization review organizations, and similar organizations for possible participation in our review. Indemnity insurers told us that they do not carry out research on the fee-for-service portion of their business, noting the limitations of existing data on medical care received on a fee-for-service basis. They often do not know the identities of family members of subscribers. They also pointed out that claims are often filed under one policyholder number, and as a result, the care received by one individual cannot be separated from the care received by another for purposes of analysis. The utilization review organizations that we contacted stated that their activities only cover utilization patterns for specific individuals, which they do not classify as research.

We interviewed representatives of the 12 organizations that participated and, to the extent available, reviewed their policies for safeguarding identifiable medical information. However, three organizations did not provide us with these policies. In addition, we did not verify the

information received from the nine other organizations. Although the organizations identified their procedures to us, we did not assess the implementation of those procedures. Because of the small number of organizations included in our study, the information we collected is not generalizable to the health care industry as a whole. Further, four organizations we contacted were unwilling to participate in this study.

In addition, we obtained information from seven IRBs. Five of these IRBs were at institutions that conduct research for the federal government, and two are freestanding IRBs that are hired for their services. Again, because of the small number of review boards in our study, the information we collected from IRBs is not generalizable. We conducted our work between July 1998 and February 1999 in accordance with generally accepted government auditing standards.

Major Contributors to This Report

Marcia Crosse, Assistant Director, (202) 512-3407
Nancy Donovan, Evaluator-in-Charge, (202) 512-7136
Donna Bulvin, Senior Evaluator
Roy Hogberg, Senior Evaluator
Gloria Taylor, Senior Evaluator
Barry Bedrick, Associate General Counsel
Dayna Shah, Assistant General Counsel
Mary Reich, Senior Attorney
Karen Sloan, Writer

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