The American Journal of Bioethics

ISSN: 1526-5161 (Print) 1536-0075 (Online) Journal homepage: http://www.tandfonline.com/loi/uajb20

"You Don't Know Me, But …": Access to Patient Data and Subject Recruitment in Human Subjects Research

Toby Schonfeld , Joseph S. Brown , N. Jean Amoura & Bruce Gordon

To cite this article: Toby Schonfeld , Joseph S. Brown , N. Jean Amoura & Bruce Gordon (2011) "You Don't Know Me, But …": Access to Patient Data and Subject Recruitment in Human Subjects Research, The American Journal of Bioethics, 11:11, 31-38, DOI: 10.1080/15265161.2011.603794

To link to this article: http://dx.doi.org/10.1080/15265161.2011.603794

Published online: 02 Nov 2011.

The American Journal of Bioethics, 11(11): 31–38, 2011

ISSN: 1526-5161 print / 1536-0075 online
DOI: 10.1080/15265161.2011.603794

Target Article

"You Don't Know Me, But . . .": Access to Patient Data and Subject Recruitment in Human Subjects Research

Toby Schonfeld, Emory University, Center for Ethics
Joseph S. Brown, University of Nebraska at Omaha
N. Jean Amoura, University of Nebraska Medical Center
Bruce Gordon, University of Nebraska Medical Center

Recruiting subjects to participate in a research study is the first step in the consent process, and therefore falls within the purview of the institutional review board (IRB) (Huntington and Robinson 2007; Neff 2008). It is a common practice to screen patients' medical information to ensure that recruitment efforts are targeted to the appropriate individuals, a practice permitted under the Heath Insurance and Portability and Accountability Act (HIPAA) preparatory research provision (U.S. Department of Health and Human Services 2003). However, this practice raises some privacy concerns. There is a clear tension here, between the needs of investigators to recruit subjects sufficient to the conduct of scientifically valid research (Ness 2007; Sataloff 2008; Wolf 2006) and the rights of patients to have their information protected.

Issues of patient privacy in screening and recruitment apply regardless of the regulatory framework. The Council for International Organizations of Medical Sciences (CIOMS) International Ethical Guidelines for Biomedical Research Involving Human Subjects, for example, describe the sanctioned use of epidemiological and other data without obtaining informed consent (p. 75). Yet we have chosen to frame our discussion within the scope of research practices and regulations in the United States for two reasons. First, the U.S. system is so large that small risks are magnified by sheer repetition. Second, the U.S. regulatory system (and HIPPA especially) has several particular shortcomings that illustrate our general concerns.

In this article, we argue that maintaining a patient's right to privacy is an essential factor in determining who has legitimate[1] access to patient information. Our thesis is that access to patient information for recruitment or screening for research must not violate a patient's privacy. That is, we argue that HIPAA's permissibility, while perhaps pragmatic, unethically expands the number of people with access to private patient information. We contend that the only legitimate access that health care providers have to private information is through the authorization granted to them by patients to provide clinical care to them. Access to this private information for *research purposes* can be granted only by IRBs that have considered the risks of what is essentially a waiver of consent against the legitimate ends of those engaged in the research enterprise.

The notion of patient privacy is motivated by at least two core Belmont principles: beneficence and respect for persons. That is, we grant privacy both to protect patients from the harms associated with others knowing their personal health information (beneficence) and because individuals have a right to determine the use of their person and personal data (respect for persons). However, we direct the bulk of this article to arguments motivated by beneficence for several reasons. First, we believe that the largest concerns about the current system are based on possible harms to patients. That is, we argue for both individual level harm and systemic harms that are the result of inappropriately broad disseminations of private health data. Second, in this article we are focusing on screening and recruitment of potential subjects. In most cases, participants will have to consent directly for data use and collection (the exception being chart review studies), and in this way the participant

1. We have elected to use the term "legitimate access" as opposed to the more common term "ethical access" because ethical access has been used so many ways with quite different meanings. Thus, we utilize a more neutral term that reflects or concern with the appropriateness of the access.

Address correspondence to Toby Schonfeld, Emory University, Center for Ethics, 1531 Dickey Drive, Atlanta, GA 30322, USA. E-mail: toby.schonfeld@emory.edu

retains control over his or her information. Limiting the discussion to the context of screening information for approach to participate in studies severely limits the scope to which the information is being used and, we contend, correlatively limits the relevance of respect for persons for this discussion. Further, we note that our argument leads to recommendations that will be generally more restrictive in the use of patient data for screening and approach. To the extent that there are additional concerns derived from respect for persons, they would presumably result in a more restrictive schema than the one we are proposing. Given that the conduct of research is also motivated by beneficence, we would suggest that we approach greater restrictions cautiously and only after implementing the proposed privacy protections.

Regardless of the motivating argument, there are significant implications of our proposal: Several current research practices permitted without IRB review and in accordance with HIPAA would be unacceptable. We detail these examples to demonstrate how closing the loophole in the HIPAA Privacy Rule would better respect patient privacy but will also likely require a sea change in current practice.

Finally, as mentioned earlier, please note that our considerations are limited solely to identifying potential research participants. Once individuals have been identified as potential subjects, then all of the typical procedures for obtaining consent to participate in research apply. Further, we note that our remarks apply only to access to information that contains personally identifiable information, and not to large data sets or other de-identified data.

THE PRIMACY OF PRIVACY: REGULATIONS AND THEIR LIMITATIONS

In the contemporary context, any discussion of privacy in health care in the United States begins—and often ends—with reference to "HIPAA." The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was expanded to include the Privacy Rule that went into effect in 2003 (U.S. Department of Health and Human Services 2003). The Privacy Rule functions to reinforce the notion that the information in a patient's record belongs to that patient, so providers are required to present patients with information about how their information will be protected for treatment, payment, or as part of health care operations (see 45CFR164.520). As a result, when patients enter a health care facility and consent to treatment, they are implicitly consenting to the privacy protections afforded by that provider.

HIPAA also has provisions regarding research. The preparatory research provision of the HIPAA Privacy Rule permits covered entities to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment. The preparatory research provision allows a researcher to identify prospective research participants for purposes of seeking their authorization to use or disclose protected health information for a research study. Therefore, covered health care providers and patients may discuss the option of enrolling in a clinical trial without patient authorization, and without IRB or privacy board waiver of the authorization.[2]

The HIPAA preparatory to research provision covers reviews of protected health information (PHI) prior to research. The actual conduct of research (beginning with the identification and recruitment of potential subjects) is governed by another section of the Code of Federal Regulations, namely, the Common Rule ("Basic HHS Policy for Protection of Human Research Subjects"). Regarding privacy, the Common Rule requires that IRBs assure that "there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data" [45 CFR 46.111(a)(7)], but offers no further definition. These regulations are what lead IRBs to require investigators to specify their procedures for recruiting and identifying potential subjects, as well as maintaining the security of data collection and storage, especially in situations where subjects are particularly vulnerable to loss of confidentiality.

When juxtaposed in this way, the curiosity of the federal regulations becomes apparent. The regulations offer two different levels of protection for the very same action, depending on when that action is carried out: "preparatory" to research or during the conduct of research itself. We contend that this regulatory distinction is not meaningful in practice. Consider that the risk/benefit calculus suggests that, if anything, reviewing private information about potential subjects prior to beginning research may in fact pose greater overall harms. Even if the risks remain the same, the benefit might be lower in that the proposed research may turn out to be impracticable, flawed in some significant way, or simply not funded and therefore never conducted. In those cases, there was risk to potential subjects with no possibility for benefit. As a result, we argue that the standard for legitimate access to this private information must be at least as high for activities preparatory to research as during its actual conduct; HIPAA creates an ethically unjustified lower standard for subject privacy protection.

Throughout this article, we do not distinguish our considerations about legitimate access to private patient information by whether they occur prior to the conduct of research or during the research process itself (which we view as beginning with the IRB application). Since we reject this distinction on ethical grounds, our arguments about the protection of patient privacy cover the research enterprise broadly. Such an approach results in the fact that in most cases our framework is *more* restrictive than both HIPAA and the Common Rule regulations, not less. Regardless, while federal regulations play an important role in privacy considerations, they are only one piece of a rather complex puzzle.

2. We note that the wide latitude provided by HIPAA in this context is in curious contrast to HIPAA's effects in clinical care. In the clinical realm, HIPAA significantly increases a patient's privacy protections, whereas in the preparatory to research realm, there exists a loophole that permits wide access to private patient information.

PRIVACY OF PATIENT INFORMATION IN CLINICAL CARE

There is no question that a clinical relationship provides health care providers with legitimate access to patient information; patients interact with health care providers for purposes of treatment, and this relationship carries with it a necessary transfer of information for the provision of services (Weber 2000). This is true regardless of the model of provider–patient interaction to which one subscribes, as the models primarily detail how the information will be used in the encounter (for more information, see Childress and Siegler 1984; Emanuel and Emanuel 1992). Virtually all provider–patient interactions involve the transfer of intimate information about physical, psychological, or spiritual structure, function, or behavior that caused patients to seek help in the first place. Patients permit their physicians to have access to this personal information about them and to gather data about their condition in order to receive appropriate care; clinic nurses and, to a more limited extent, clerical personnel also have necessary access to these data (Siegler 1982).[3] Along these same lines, courts have ruled that limited intrahospital communications between care providers and hospital counsel that include patient information do not violate the patient's right to privacy (Kern 2002).

Yet such disclosure of information puts patients at a potential risk of harm should that information be shared with third parties; studies have demonstrated that patients are just as worried about information being shared with members of their social community as being shared with their employers or an insurance company learning about private information (Sankar 2003). In response to these concerns and misunderstandings about their regulatory protections, patients take independent action to avoid disclosure, such as withholding vital information or failing to seek help in the first place; this is a particular concern for those who feel they are at high risk for disclosure, such as those with or at risk for HIV infection, adolescents, those with mental health issues, and female victims of domestic violence (Sankar 2003). As Ken Kipnis helpfully points out, the professional value of maintaining medical confidentiality is the best, albeit imperfect, safeguard for protecting vulnerable parties from the harm that may result from unwarranted disclosure (Kipnis 2006).

Therefore, patients grant extended but limited approval to health care providers to have access to their private information. The circle of those with permission to have access to private patient information is partly determined by patients themselves (by choosing the provider to see etc.) and partly determined by the institution or organization of which that provider is a member (teaching hospital etc.).

Because of the current composition of the health care system, individuals unknown to the patient are likely to have legitimate access to patient private information. For Doctor X to diagnose and treat correctly the problem of Patient A, additional health care personnel such as phlebotomists, radiology technicians, and others may have to review Patient A's data. However, none of this constitutes a breach of privacy. Rather, to the extent that the other personnel contribute to Doctor X's ability to care for Patient A, their access to private patient information has been approved by the patient, either explicitly through the admissions process, or implicitly through the notification of the institution's privacy policy (provided that the patient still presents for care after reviewing the policy).

These kinds of authorizations also can transfer vertically or horizontally. In teaching institutions, vertical transfer is common: The patient may have seen the resident[4] exclusively for her care, but it is ultimately the attending physician who is responsible for that care and no violation of privacy exists when the resident communicates information to the attending physician about the patient's care. Horizontal transfers of information can happen in group practices, where providers cover each others' practices at night, on weekends, or at other off times in order to provide continuing service. The same is true for hospital service. Dr. Y may only be "on service" at the hospital every third week, which virtually guarantees that patients on her service will also see one of her partners in the meantime.

If we grant that a great many individuals have legitimate access to patient information for the purposes of clinical care, does it necessarily follow that they also have legitimate access for the purposes of research? To answer this question, we must first elaborate on the notion of privacy of health care information.

PRIVACY OF INFORMATION

Even if one were to grant that all the individuals discussed earlier have legitimate access to private health information for clinical purposes (by virtue of the patient's explicit or implicit permission), does that access automatically extend into the domain of research for which the patient has granted no such permission? We contend that, to a limited extent, it does. The foundational principle here is the consideration of the potential harms that might be conferred on patients if access were unrestricted. We believe these risks fall into two categories: (1) the risk of confidentiality breach that results in wider distribution of information that could damage the individual patient/participant, and (2) the more general harm of patients acting to protect their own privacy by failing to provide full information to physicians. In both cases, to the extent that a clinician-investigator already knows private information about a potential research participant, there is no expansion of the patient's privacy and therefore no harm is conferred. The argument goes as follows:

1. The rationale for limiting access to a patient's information in the *clinical* context is that the patient reserves the right to authorize or not to authorize the release of

3. For example, the receptionist needs to know why I want to see the doctor in order to schedule me in an appropriate slot.

4. Or student, or intern, etc.

his or her private health information.[5] Granting access to patient information may result in dissolution of the notion of privacy, which could have many untoward effects including both individual level harms (from the wider circulation of information that harms individuals) and collective harm (e.g., breach of patient trust, failure of patients to communicate openly or to seek help in the first place from health care providers, etc.; Edwards 1988).

2. If the proposed researcher already has a clinical relationship with the patient such that he or she has legitimate access to the patient's clinical information, no expansion of access to private health information is required in order for the researcher to screen the patient for inclusion or to strip identifiers. As a result, there is no information leakage when information the individual already has is used for research.

   Consider why this is so: all of the harms mentioned in (1) result from an unsanctioned expansion of those with information about the patient: more people would know private information. However, the clinician-researcher does not fall into this category: He or she *already* knows the private information about the patient that is relevant to the research purposes. We readily grant that using this information for research without the patient's consent is both unethical and a violation of regulations, but preexisting knowledge of this information could form the basis for approaching the patient to obtain consent to participate in research. Worries about *potential harm alone* cannot justify excluding access to the patient's information as a method of screening potential research subjects.
3. Therefore, based *solely* on the notion of maintaining patients' privacy rights, if a researcher has legitimate access to a patient's information for clinical purposes, he or she also has legitimate access to that patient's information for identifying potential research subjects.

Note that this argument is based entirely on the notion of privacy. However, there may be other ethical considerations motivated by respect for persons—such as the purpose to which the information will be put, and so on—that are part of the calculus regarding ethical access. As noted earlier, such considerations are generally more restrictive of researchers than the notion of privacy motivated by beneficence itself. Our purpose here is to begin the discussion of legitimate access to patient information by focusing on the concept of privacy, and we leave for future research the question of additional, perhaps more restrictive, criteria for access to patient information.

Who's In, Who's Out

If, in fact, the key moral distinction is the notion of privacy rights, then it seems that anyone whose job has required him or her to have access to private patient data will fall within the scope of "approved" individuals—those with legitimate access to the patient and/or patient's information for identifying potential research subjects. This is because these individuals already know private information about the patient for clinical reasons, so there is no violation of patient trust in knowing that information for research purposes.

The next step is to determine who will fall into the "acceptable" realm and who will not: that is, which providers will be granted access to the patient for research recruitment purposes and which ones will be denied? Data demonstrate that some sites restrict the screening of records to health care professionals within an office practice, some include office staff, and other sites permit an external research assistant to perform this task. We have reflected on these data, and put some common agents to the test to see in which camp they will fall according to our criterion of minimizing violations of patients' privacy.[6]

- *Partners of the health care provider*: Access to patient information for this group of individuals requires actual, not potential, interaction with the patient's clinical situation. It is not enough to say that Doctors X, Y, and Z are in practice together, and that Patient A *could have* seen Doctor Z if she had had a problem during the week of Doctor X's vacation. Rather, only if Doctor Z *actually* cared for the patient is informational access granted for research purposes. If Doctor Z has not actually used this information (and thus becomes aware of it) through approved clinical practice, then Doctor Z's perusal of this information for research screening has increased the number of people who know the patient's private information without the patient's permission and as a result may have subjected the patient to harm.

  Note that this access is granted regardless of whether or not the patient is aware of this contact. Suppose the patient calls her physician's office with a complaint of symptoms consistent with a urinary-tract infection. If Doctor X is on vacation that week, the nursing staff will consult Doctor Y about the problem and make a recommendation based on that (come into the clinic, call in a prescription, etc.). Patient A may have had no direct contact with Doctor Y, but Doctor Y still cared for Patient A: she reviewed her chart, considered her symptoms, and so on. Because she had legitimate access to Patient A's information for clinical care, Doctor Y retains that access for research, *even if that research does not address the reason for the clinical care*. Suppose that during the chart review, Doctor Y sees that the patient has been treated for *Chlamydia* recently. Doctor Y is doing a study on patients with *Chlamydia*. Given

5. HIPAA makes certain provisions for treatment, payment, and health care operations without patient authorization, but here we are specifically referring to the patient's dominion over his or her health information.

6. Please note that the considerations offered here do not address studies that include large de-identified data sets. Our concern is with harms that may be conferred on patients as a result of additional individuals knowing their private information. These harms do not, and cannot, arise when information has been de-identified and therefore cannot be linked back to the original participant.

that she discovered through her (albeit brief) clinical relationship with the patient that she may fit the inclusion criteria of her *Chlamydia* study, there is no harm to the patient if Doctor Y uses that information in order to determine whether the patient is eligible for a given study.

- *Specialist consultant*: As in the case of the partner just described, the specialist with whom the primary provider consults, whether formally or informally,[7] to assist her in the care of the patient also has legitimate access to private patient information. Because this provider already had access to the patient's private information (and learned, for example, that the patient has hepatitis C, for which the provider is conducting an observational study), no expansion of the scope of individuals aware of the patient's private information occurs, and, therefore, the patient is not harmed.
- *Quality assurance team*: Quality assurance (QA) or improvement practices are a regular part of the health care system. Data are routinely analyzed to ensure that a variety of practices or procedures are continuing to produce results of value. These QA projects can be institution-wide (as with patient satisfaction surveys) or can be discipline specific (like weekly morbidity and mortality sessions for a particular clinical department). It is true that in order for these processes to work adequately, detailed patient information is required. However, rarely is it necessary that identifiable private information about a patient be disclosed for the conduct of the discussion. For example, it might be important to see the patient's x-ray, but it is likely to be unimportant to see the patient's name or Social Security number on the film. Or it might be important to know that the patient was from rural Nebraska, but unlikely to be important to know that she is the only certified librarian in all of North Platte. The idea is that information that links a patient's identity to information about that patient is not necessary in order for this job to be done and done well. Therefore, while it sometimes happens that those doing QA have default access to patient identifiers, we argue that since there is no clinical necessity for this information, there can be no research authorization without violating the patient's privacy rights. Therefore, we argue that individuals doing QA do *not* have legitimate access to patient information for research purposes.
- *Research nurse/coordinator*: Many investigators use grant or other funds to enable the hiring of a research nurse/coordinator to assist with conducting the study. While the investigator remains ultimately responsible for the conduct of the research, it is often the research nurse/coordinator who handles the daily operations of the study. This role makes the research nurse/coordinator particularly knowledgeable about study procedures, and is an excellent resource for those who have questions about the study. Partly because of this unique role, and because this person often has past experience working with patients for clinical care, the research nurse/coordinator is often involved in the consent process.

  However, given the potential for harm we described earlier, it is not at all clear that the initial screening is within the research nurse/coordinator's rights to access information. We previously argued that only those with *prior* access to patients' private information for clinical purposes had access for research purposes. This is to minimize the harm that might befall patients by an expansion of the circle of those with access to sensitive data. Unless the research nurse/coordinator has had access to the patient's information through clinical practice, we would argue that this person does *not* have legitimate access to private information prior to a potential subject's consent. Special permission must be granted by the patient in order to give the research nurse/coordinator such access. This permission may be achieved simply: The physician or someone else with legitimate access can say to the patient, "We are doing a study on people with rashes like yours. Would it be ok if a research nurse came in to tell you about the study (or reviews your file to determine eligibility)?" If the patient acquiesces, then the research nurse can approach the patient or search his or her medical record. But if the patient's answer is no, even to a query about searching the patient's information in a database or chart, then the door is closed to the research nurse/coordinator.
- *Physician's secretary:* What about someone who lacks a clinical relationship with the patient, but who has legitimate access to the patient's private information for purposes of clinical care? For example, a commonly used drug regimen has been recalled by the manufacturer. Dr. X has her secretary send letters to all of her patients taking Drug Q to notify them of this change. This function is part of the delivery of health care, and therefore this falls within the prior authorization the patient has given her physician to care for her. However, now suppose that the physician asks her secretary to type and send out letters inviting patients to participate in a study on her behalf. Patients who have been in remission for 6 months or more are eligible. In order to gather these data, the secretary would need to know private information about patients for something other than clinical care.

  In this instance, where the letter is for research and not clinical care, we argue that the same principles hold as were discussed earlier regarding the partner of the treating physician. To the extent that the secretary would have to acquire new private information about patients in order to fulfill this research goal, this practice constitutes a breach of privacy. If, on the other hand, the secretary has had prior access to these particular patients' information, then sending the letters does not constitute a breach of privacy. For example, suppose this is a small medical

7. Note that for enforcement purposes, IRBs may find it difficult to regulate practice unless the consultation is formal, and thus documented in the medical record. However, for purposes of privacy considerations, the consultant need not be formally engaged in the patient's care as long as he or she obtained the private information about the patient through actual clinical care.

practice where this single secretary handles all patient records. In that case, gathering the data for the research would not lead to additional knowledge. Or suppose that the secretary in question has previously sent a clinical letter to every patient who is to be invited into this research study; again, there would be no expanded access of information. Regardless, the key notion here is whether or not additional information must be gathered in order for the secretary to perform his or her task in research; if the answer is yes, then privacy concerns dictate that the secretary does not have legitimate access to these data.

PRACTICAL CONSIDERATIONS FOR THE CONDUCT OF RESEARCH

From the argument thus far, it might appear that access to potential subjects and the conduct of research would be severely restricted. This is because it looks like only health care providers themselves would be able to screen patients for subject inclusion, or even address the letters to potential subjects inviting them to consider participation in a study. This would bring the research enterprise to a grinding halt.

However, obtaining patient permission in these situations need not be overly cumbersome. A clinical provider with whom the patient has a clinical relationship can provide the introductions for the new person. A sample script may go as follows: "I am doing a study on people with rashes like yours. Would it be ok if I had Suzy, our research nurse, come in and talk with you about the study?"

Another suggestion would be for the provider or a member of the provider's team (nurse, etc.) with whom there exists a clinical relationship to present the study to the patient. After the patient agrees to participate, then associated study personnel can be involved. This is because there is no breach of privacy here, nor any perception of a breach: the patient has given her or his specific consent for others to know information for the specific purpose of research.

It might even be possible in the course of a routine visit for a physician to obtain some sort of blanket permission from patients, where the patients agree to be approached by a researcher or to have their records screened whenever their physician thinks they might be eligible for a study. Note that here we suggest a "blanket" permission to be screened and approached for recruitment into a suitable study, *not* as a substitute for a robust consent process, which would happen once a potential subject has been identified.

However, there may be circumstances in which these options will not be feasible, and researchers are left with no easy way to have access to potential participants. In these instances, investigators and IRBs must balance considerations of privacy (respect for persons—enabling a patient to decide how to limit access to his or her information) with beneficence-based considerations (conducting important research to improve the health of many patients). The question is, then, whether or not there is precedent for balancing competing interests in research.

We hold that provisions for waiving informed consent in research presents just such a precedent.[8] In fact, one could argue that giving an investigator access to information is simply an example of waiving informed consent. Federal regulations describe the necessary elements for obtaining informed consent from a research participant or his or her legally authorized representative (45 CFR 46.116). However there are some instances where consent can be waived under these regulations.[9] These instances include when (45 CFR 46.116(d)):

1. The research involves no more than minimal risk to the subjects.
2. The waiver or alteration will not adversely affect the rights and welfare of the subjects.
3. The research could not practicably be carried out without the waiver or alteration.
4. Whenever appropriate, the subjects will be provided with additional pertinent information after participation.

The classic example of a research study where consent might be waived is research involving deception. Consider a study where investigators are interested in subjects' response to a particular injustice. In this case, obtaining consent of subjects prior to conducting the research would fundamentally change the way the subject reacted to that injustice, thus making the results invalid. For this reason, obtaining traditional informed consent would be impracticable—or, in fact, impossible. Yet the impracticability of obtaining informed consent is not enough. Investigators would have to demonstrate to the IRB why the information collected from this study could not be obtained in another way, without deception. Provided that the information could not be collected without deception, participants would be provided information about the real purpose of the study after participation. In this way, their rights and welfare would not be adversely affected. Note, however, that an IRB would only approve such a waiver of informed consent if the risk to subjects were no more than minimal. A study where investigators were interested in subjects' response to sudden and intense physical pain, for example, would violate the requirement that the research involve no more than minimal risk.

We contend that similar considerations should apply to the notion of access to a patient's private information. The potential risk in question relates specifically to the privacy of a patient's information: The release of information has the potential to harm the subject in some way (i.e., insurance companies raising policy premiums, risk of domestic

8. We acknowledge that the Food and Drug Administration (FDA) does not have a provision for waiver of consent, so there is no parallel for FDA-regulated research. However, we contend that it is unlikely that such research would meet the criteria for waiving of consent in the first place. In these instances, investigators will have to rely on those with legitimate clinical access to patient information to secure patient consent before screening them for research purposes.

9. The CIOMS Guidelines contain similar criteria; see CIOMS (2002).

violence, or simply shame or embarrassment). The magnitude of this harm must be no greater than minimal in order for an expansion of ethical access to be granted. Finally, investigators must be able to demonstrate that the rights and welfare of subjects in the study would not be adversely affected by the release of information. If the logistics of a particular study precluded the suggestions we made earlier, and if the release of this information posed no more than a minimal risk to subjects, then legitimate access could be extended further than what we argued in the previous section by waiving consent to access patient information.

For instance, if a study were conducted where the screening information simply required knowing that the subject had had a pap smear in the past 6 months, an IRB might reasonably grant access for screening purposes to a research nurse hired by a physician-investigator. Pap smears are part of routine clinical care and are not indicative of any particular medical condition. As a result, the release of the information that a particular patient had a pap smear (not the results of the test) appears to present harm no greater than minimal risk. Because of this, the rights and welfare of the subject are not adversely affected by the release of this information.[10]

On the other hand, if a study were conducted where the screening information required knowing that the subject had a history of HIV diagnosis in the past 6 months, the potential for harm associated with the release of the information is much higher and therefore likely greater than minimal risk. Release of data about HIV infection could result in harms such as insurance, social, or economic discrimination, embarrassment, etc., and therefore the release of the information would adversely affect the rights and welfare of the subject. In cases such as this, granting expanded access to patient information would not be ethically permissible.

All of this is predicated on the notion that the research, in addition to posing no more than minimal risk to subjects, is also impracticable to be done in any of the ways suggested earlier. *Both* the impracticability *and* the magnitude of harm must be justified to an IRB for an expansion of ethical access to be considered acceptable.

PUTTING THE ARGUMENT IN PERSPECTIVE

It might appear that the previous section provides investigators a way to circumvent the regulations that protect subjects' privacy. This is not our intention. We note that most of our suggestions require a change in practice that enables subjects to have more control over their own information. We stress that the third solution (waiver of consent) is listed only as a rarely used mechanism, and should be considered by the IRB on a case-by-case basis. The level of risk clearly differs from study to study and can only be determined by the IRB based on the particular information that is being sought in the screening process. Thus, we would contend that a standing policy or blanket waiver would be inappropriate.

The *only* time that the waiver of consent should be considered is for studies where, for some unforeseen reasons, our other suggestions could not be applied. In addition, for the proposed study, the likelihood of benefit must be so high, and the risk so small, that additional mechanisms are required for obtaining legitimate access to patient information.

CONCLUSION

The process for acquiring information prior to research needs to more closely mirror conduct during research. We recognize that implementing such a standard would require a significant change in current practice, both in regard to work preparatory to research and in the conduct of research itself. Yet we have offered practical suggestions as to ways to continue to meet the needs of researchers while still protecting the privacy rights of individuals. ■

10. We take "adversely affecting the rights and welfare" to be a term of art. Taken literally, it would prevent the waiver of consent under any circumstances; the waiver of consent itself adversely affects the rights and welfare of the subject. Therefore, we take it to mean that the IRB should use its judgment to prohibit screening of information that a reasonable person would likely find to be particularly sensitive (i.e., a diagnosis of *Chlamydia*).

REFERENCES

Childress, J. F., and M. Siegler. 1984. Metaphors and models of doctor–patient relationships. *Theoretical Medicine* 5(1): 17–30.

Council for International Organizations of Medical Sciences. 2002. *International ethical guidelines for biomedical research involving human subjects*. World Health Organization, Geneva. Available at: http://www.cioms.ch/publications/layout_guide2002.pdf (accessed January 28, 2011).

Edwards, R. B. 1988. Confidentiality and the professions. In *Bioethics*, ed. R. B. Edwards and G. C. Graber, 72–81. Chicago: Harcourt Brace Jovanovich.

Emanuel, E. J., and L. L. Emanuel. 1992. Four models of the physician–patient relationship. *Journal of the American Medical Association* 267(16): 2221–2226.

Huntington, I., and W. Robinson. 2007. The many ways of saying yes and no: Reflections on the research coordinator's role in recruiting research participants and obtaining informed consent. *IRB: Ethics & Human Research* 29(3;3): 6–10.

Kern, S. E. 2002. Privacy: Intrahospital communications regarding patient care held constitutional. *Journal of Law, Medical & Ethics* 30(1): 112–114.

Kipnis, K. 2006. A defense of unqualified medical confidentiality. *American Journal of Bioethics* 6(2): 7–18.

Neff, M. J. 2008. Informed consent: What is it? Who can give it? How do we improve it? *Respiratory Care* 53(10): 1337–1341.

Ness, R. B. 2007. Influence of the HIPAA Privacy Rule on health research. *Journal of the American Medical Association* 298(18): 2164–2170.

Sankar, S. P., S. Mora, J. F. Merz, and N. L. Jones. 2003. Patient perspectives of medical confidentiality: A review of the literature. *Journal of General Internal Medicine* 18(8): 677–678.

Sataloff, R. T. 2008. HIPAA: An impediment to research. *Ear, Nose & Throat Journal* 87(4):182, 184.

Siegler M. 1982. Sounding boards. Confidentiality in medicine—A decrepit concept. *New England Journal of Medicine* 307(24): 1518–1521.

U.S. Department of Health & Human Services, Office for Civil Rights. 2003. *OCR privacy brief: Summary of the HIPAA Privacy Rule*. May. Available at: http://www.hhs.gov/ocr/ privacysummary.pdf

U.S. Department of Health & Human Services, Office of Human Research Protections. 2005. *45 Code of Federal Regulations, Part 46: Protection of human subjects* (June 23). Available at: http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm (accessed July 10, 2009).

Weber, L. 2000. Access to medical information: 10 Ethical guidelines. *Clinical Leadership & Management Review* 14(6): 280–284.

Wolf, M. S., and C. L. Bennett. 2006. Local perspective of the impact of the HIPAA privacy rule on research. *Cancer* 106(2): 474–479.