



Via email and fax

Captain Michael A. Carome, M.D.
U.S. Public Health Service
Office for Human Research Protections
1101 Wootton Parkway, Suite 200
Rockville, MD 20852

Re: Comments regarding OHRP Human Subjects Protection, Training, and Education; 73 Fed. Reg. 37460-63

September 22, 2008

Dear Captain Carome:

The World Privacy Forum appreciates the opportunity to comment on the Office for Human Research Protection's (OHRP) request regarding implementation of human subjects protection training and education programs. The notice appeared in the Federal Register on July 1, 2008 at 73 Fed. Reg. 37460-63. The World Privacy Forum is a non-partisan, non-profit public interest research and consumer education organization. Our focus is on conducting in-depth research and analysis of privacy issues, in particular issues related to information privacy and health privacy. More information about the activities of the World Privacy Forum is available at <<http://www.worldprivacyforum.org>>.

In general, the World Privacy Forum believes that there is a substantial need for better and more systematic training for members of institutional review boards, or IRBs. This need is well-documented in the studies and investigations that OHRP cited in the notice, as well as in other literature.¹ Our own experience with the research community suggests that knowledge about privacy is thin and that IRBs appear to be neither uniform in approach nor adequately equipped to address privacy issues that arise in the course of research projects.

Although IRBs do not intend to be deficient in their knowledge and do not intend to exercise weak oversight in the area of privacy, the result is nevertheless the same. The research community is too often lacking in basic expertise about and concern for privacy, which has led to

¹ See, e.g., Sharona Hoffman, *Regulating Clinical Research: Informed Consent, Privacy, and IRBs*, 31 Cap. U.L. Rev. 71 (2003).

a number of mishaps and shortcomings.² One example among many possible examples of a lack of in-depth knowledge relates to the HIPAA health privacy rule. HIPAA does not equal privacy, but too often IRBs do not seek to go beyond basic HIPAA compliance. While concern about HIPAA is welcome, HIPAA was never designed to function as an omnibus privacy protection scheme for research.

Our comments focus on the types of training and materials that are needed and that would be appropriate for IRB members. Our focus is exclusively on privacy matters. The World Privacy Forum has no position on other issues relating to IRB training or on whether better training should be accomplished through mandatory regulations.

The OHRP posed these questions:

(3a) Should further guidance or a regulation include provisions stipulating specific content for the training and education programs? If so, what should the specific content include and why?

We offer three different areas for subject matter training and for the types of materials that would be most helpful to researchers and most protective of research subjects.

I. HIPAA and Other Privacy Standards

The research community has not been shy in criticizing the HIPAA health privacy rule for its effects on the conduct of health research.³ While there have been some transitional problems with the rule, many of the reported problems are the result of ignorance, local policies not required by HIPAA, or over compliance with HIPAA requirements. If everyone involved with the disclosure of health records for research were better informed about the actual content of the health privacy rule, much of the complaining would likely disappear or be properly focused on the responsible parties. We do not believe that the HIPAA rule is perfect by any means, but many of the complaints aimed by researchers at HIPAA would be more properly targeted at others or are off base. Researchers are not exempt from the obligation to protect the privacy of individuals who are their data subjects.

The research community lags behind the general health community and even significant parts of the commercial sector in awareness of and compliance with general privacy standards. Prior to

² See Department of Health and Human Services, Office of Inspector General, *Review of Corrective Actions Concerning the Human Subject Research Program* (2006) (A-06-06-00042) <<http://oig.hhs.gov/oas/reports/region6/60600042.htm>>.

³ For a summary of heated warnings from researchers regarding how HIPAA would stand in the way of research, see Mary L. Durham, How Research Will Adapt to HIPAA: A View from Within the Healthcare Delivery System, 28 AM. J.L. & MED. 491, 492 (2000). See also Association of American Medical College's Statement before the National Committee on Vital and Health Statistics on Standards for Privacy of Identifiable Health Information, Final Rule," (August 2001), <<http://www.aamc.org/advocacy/library/hipaa/testimony/2001/082201.htm>>. See also: Jennifer Kulynych & David Korn, *The Effect of the New Federal Medical-Privacy Rule on Research*, 346 N. Engl. J. Med. 201, 201-04 (2002).

HIPAA, health care providers mostly paid lip service to privacy, but few devoted substantial resources to privacy. Privacy policies were scarce, and privacy training for staff was largely unknown. For health care privacy, HIPAA produced a sea change. The commercial sector – especially that segment engaged in Internet activities – has also changed in the past decade as a result of legislative pressure and marketplace demands. Many if not most commercial websites today have privacy policies.⁴

The research community – except perhaps for those that are covered entities under the HIPAA health privacy rule – stands today in the same approximate place health care providers were before HIPAA. Privacy for many researchers is viewed as an annoyance rather than accepted as an integral part of the research process. Indeed, the research community may be guilty of the same degree of inattention to privacy that it had for human subjects protection in general prior to the Belmont Report and the Common Rule.⁵

Privacy is not a significant barrier to research. We observe that health researchers in the EU Member States function under more comprehensive privacy rules that apply not only to record holders, but to the researchers themselves.⁶ In the United States, researchers at federal agencies have operated for more than 30 years under the requirements of the Privacy Act of 1974 with few reported problems or complaints.

We have several suggestions for training and materials that would be helpful for researchers and for IRB members. Our focus on researchers as well as IRB members is intentional, because a rising privacy tide will lift all boats. We also suggest that basic materials on privacy be prepared by or funded by OHRP. There is no reason to ask multiple institutions to develop resources that can be used by all.

HIPAA Privacy Standards:

Researchers and IRB members involved in health research using records subject to the HIPAA health privacy rule should have a complete understanding of the rule's standards. They should be able to readily determine whether a particular institution's privacy requirement is due to the HIPAA rule or to another standard,

⁴ The California Online Privacy Protection Act of 2003, <<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579>>, requires many commercial web sites to post a minimal privacy policy. This law has had the effect of reinforcing the standard practice of posting a privacy policy on a corporate home page. In 2008, privacy NGOs used this law to pressure Google to add a link to its privacy policy on its home page. See Linda Rosencrance, *Privacy Groups to Google: What took you so long?* ComputerWorld, July 8, 2008.

⁵ National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, *Ethical Principles and Guidelines for the Protection of Human Subjects of Research* (1979) (Belmont Report). The Belmont Report sets out ethical human subject research principles for research involving humans. <<http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.htm>>. The Common Rule (Protection of Human Subjects), 46 CFR Part 45, incorporates the Belmont Report by reference.

⁶ European Union, Council Directive 95/46, art. 28, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281/47), <http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf>.

such as one established by a health care institution. This is not a particularly challenging requirement. It should take no more than 30 minutes for a researcher to understand the regulatory obligations. The availability of clear and easy to use reference materials will provide ongoing benefits.

Privacy Act of 1974:

Researchers and IRB members involved in health research subject to the Privacy Act of 1974 need training in the Act's requirements. Although the Act has been in place for more than 30 years, agency implementation of the Act has been consistently inadequate. Federal agencies that undertake research subject to the Act would benefit from focused training and materials on the Act's requirements. As with HIPAA, learning the requirements of the Privacy Act of 1974 takes minimal time.

Other Privacy Standards:

Other standards for privacy can be found in the Substance Abuse rules (42 C.F.R. Part 2). Ignorance of the substance abuse rules, even within the substance abuse community, is widespread. Anyone engaging in research involving substance abuse can easily become subject *directly* to the rules.

Other federal privacy rules exist that may affect research activities. For example, the U.S. Housing and Urban Development (HUD) rules for Homeless Management Information Systems (HMIS) include privacy standards that affect researchers using homeless records.⁷ The Family Educational Rights and Privacy Act⁸ regulates the disclosure of school records. State laws may also impose privacy standards for some records, including substance abuse records, genetic records, mental health records, and other categories.

We are aware that OHRP maintains an international compilation of human research protections.⁹ As impressive as this document is, the OHRP compilation is not comprehensive with respect to all federal rules affecting research (e.g., the substance abuse rules and the HMIS rules are not referenced), and it does not appear to include any state statutes or rules. OHRP could expand and enhance its compilation to cover all United States requirements. That would be an important and substantive contribution to IRBs and to researchers in general.

⁷ See <<http://www.hmis.info/Resources/312/HMIS-Data-and-Technical-Standards-Final-Notice.aspx>>.

⁸ 20 U.S.C. § 1232g; 34 CFR Part 99.

⁹ <<http://www.hhs.gov/ohrp/international/HSPCompilation.pdf>>.

International Privacy Standards:

Researchers engaged in research that involves record subject or records in other countries are likely to be subject to foreign data protection laws. The U.S. research community – which does not generally have a competent understanding of U.S. privacy rules – is surely deficient in its understanding of the privacy (and other) laws affecting research conducted across international borders. Researchers with international partners may learn something about foreign laws, but U.S. IRB members are certain to need more help. As electronic health information exchange captures more records of citizens belonging to EU countries and other countries with stronger privacy protections than the US, this may become increasingly important.

A recent example of weaknesses in the international arena can be found in the much-publicized Northeastern University “cell phone tracking” study, where researchers used cell phone records to track the movements of individuals over time.¹⁰ The study authors did not seek ethics approval or advice because they viewed the study as a physics, not a biological, study. The study was conducted overseas in a location the researchers would not disclose. A number of members of the research community and others have voiced concerns over how this study was conducted. The FCC stated that the study would have been illegal if it had been conducted in the US, and a University of Pennsylvania bioethicist noted that an ethics panel would not have been likely to approve the study. These kinds of problems are not new or unknown to DHHS, as the OIG has already reported on the growth in international human research studies and the challenges they can pose.¹¹

A laudable goal would be to avoid problematic research protocols that violate international privacy standards in the first place. While we understand that the researchers in, for example, the Northeastern study acted entirely out of bounds, we believe that better training in what standards apply to protection of human subjects (including studies that could potentially be classified as “physics” studies due to a technology cross-interest) and broader IRB understanding of international privacy standards will generally help disseminate a greater depth of understanding in this area over time in the research community.

¹⁰ See John Schwartz, *Cell phones show we're all in a rut; Call signals are used to track where people spend their days*, The International Herald Tribune, June 6, 2008. See also *Researchers from Northeastern Ignore Privacy Issues to Conduct a Cell Phone Study*, Digital Journal, June 5, 2008. See also Seth Borenstein, *Study secretly tracks cell phone users outside US*, Associated Press, June 4, 2008.

¹¹ Department of Health and Human Services, Office of the Inspector General, *The Globalization of Clinical Trials: A Growing Challenge in Protecting Human Subjects* (2001) (OEI-01-00-00190), <<http://www.oig.hhs.gov/oei/reports/oei-01-00-00190.pdf>>; see also Joe Stephens et al., *The Body Hunters*, Washington Post, Dec. 17-22, 2000.

Regretfully, problematic and potentially illegal protocols harm the entire research community by creating a lack of trust and undermining the bona fides of legitimate researchers.

II. Certificates of Confidentiality and Statutory Confidentiality Protections

The World Privacy Forum strongly supports certificates of confidentiality for research involving human subjects. We are not prepared to argue that researchers should obtain a certificate for all human subjects research, but nearly all research that involves identifiable health data or other personal data about individuals should have a certificate of confidentiality unless a researcher can state a substantive reason why a certificate is not appropriate for the study. We agree with this statement from the NIH Certificate Kiosk that “[C]ertificates of Confidentiality constitute an important tool to protect the privacy of research study participants.”¹²

Many IRB members and others in the health research community do not know about the available certificate programs. We are aware of the OHRP Guidance,¹³ but it is not enough. Indeed, 42 U.S.C. § 241(d) is not the only certificate program for research,¹⁴ and there are other statutes that address the confidentiality of records used in certain types of research.¹⁵ All of this information should be readily available from one source (with OHRP being the most likely candidate). IRB members should be trained in these statutes that protect the records of research subjects. The rest of the research community should also be made more aware of the law governing research records.

WPF recommends that all researchers be required or encouraged to consider the availability of a certificate of confidentiality and to state a reason why a certificate was not obtained. In addition, researchers should be required or encouraged to identify directly in protocols submitted to IRBs any statutory protection that applies to their activities. If there is no applicable statutory protection, researchers should so state this fact. These responsibilities could easily be incorporated in standard IRB practices.

We are aware of the substantial time pressures and lack of staffing pressures confronting most IRBs. The 2000 OIG report on IRBs indicated that many difficulties can arise from IRB’s lack of resources.¹⁶ Given this backdrop, ease of access to thoughtful and thorough privacy information is essential to making a dent in the privacy deficiencies and discrepancies in IRBs.

OHRP can help the research community increase awareness by preparing a short form with a summary of all potentially applicable research confidentiality statutes and certificate programs.

¹² <<http://grants.nih.gov/grants/policy/coc/>>.

¹³ <<http://www.hhs.gov/ohrp/humansubjects/guidance/certconf.htm>>.

¹⁴ See, e.g., 21 U.S.C. § 872(c).

¹⁵ These statutes include, but are not limited to 42 U. S.C. § 299c-3(c).

¹⁶ DHHS, Office of Inspector General, Protecting Human Research Subjects: Status of Recommendations (2000) (OEI-0197-00197), <<http://oig.hhs.gov/oei/reports/oei-01-97-00197.pdf>>.

Check boxes can make it easy for researchers to complete the form and for IRBs to conduct a review of the form. For each certificate program or confidentiality statute, a researcher would check whether it is applicable to the research project.

Researchers should also be required to identify any security breach notification laws that apply to their activities. Most states have these laws, although they may not apply to all researchers. Even in the absence of a law, researchers should be told to pay attention to moral obligations in the event of a security breach. We assume that researchers are not exempt from the incidents that give rise to security breaches, including carelessness, lost laptops, missing memory sticks, and security lapses.

With the appropriate forms and summaries of the law, the entire research community would become much more fully aware of statutory protections for research subjects (and obligations of researchers) at the conclusion of one cycle of research protocol preparation and review. OHRP could easily develop or commission a form and fact sheet at very little cost. Additional information also could be prepared to explain what researchers must do when they have certificates or when statutory confidentiality provisions apply to their research. There is no reason for this basic explanatory and reference work to be done more than once.

III. Privacy Policy Formbook

In our view, researchers and IRBs do not pay enough attention to their privacy obligations. A research project, like any other endeavor involving the collection and maintenance of personal information, should operate under a formal privacy policy. Each policy should incorporate Fair Information Practices (FIPs) as promulgated by the Organization for Economic Cooperation and Development (OECD).¹⁷ We note that there are other versions of FIPs in circulation, but the OECD Guidelines are the most widely recognized in the world.¹⁸

The main purposes of a privacy policy are to (1) explain to research subjects how their information will be processed and what rights they have with respect to the information, and (2) inform the researcher and the researcher's associates how they may process personal information. Both of these purposes are equally important.

We suspect that many, if not most, research projects do not have a written privacy policy today. A diligent researcher who wants to have a privacy policy must start from scratch. Developing a privacy policy is not difficult, but it is a challenge for those busy with other work and who are not already familiar with privacy.

A privacy policy formbook would be of great assistance to the researcher and research community. It would reproduce the principles of FIPs, offer a variety of implementation strategies for each principle, and provide language suitable for a research privacy policy. We do

¹⁷ The *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* can be found at <http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>.

¹⁸ For more on FIPs, see the history of FIPs at <<http://bobgellman.com/rg-docs/rg-FIPshistory.pdf>>.

not suggest that every research project should have the exact same policy, which is why alternatives would be appropriate.

If OHRP sponsored a privacy policy formbook, a researcher could consult the formbook, select those parts most applicable to the circumstances of the research, and have a complete policy in short order. A privacy policy formbook would also aid an IRB in overseeing the privacy policy adopted by a researcher. It would give the IRB a standard against which to measure the choices made by the researcher.

A privacy policy formbook should be drafted with full consultation of the research community, the privacy community, federal and state agencies, and the public. Where good policies already exist, they can serve as examples that can be adapted for use by others. For research projects that involve the sharing of information across national borders, the formbook can address how a privacy policy can conform to the privacy laws of other nations.

IV. Conclusion

The World Privacy Forum hopes that these comments and suggestions are helpful. If the research community had a better reputation for protecting privacy, it would probably find a greater degree of public acceptance, more willing participants in research activities, and fewer barriers to research subjects and their records. More attention to privacy would likely help researchers to achieve their substantive goals. We stand ready to assist OHRP or others in the research community to implement the ideas we have proposed.

Respectfully submitted,

Pam Dixon

World Privacy Forum
www.worldprivacyforum.org
+1 760-269-0094