IRB *EasyEd™* - For IRB Members Volume 1 Number 7

Topic: Privacy and Confidentiality

Overview of the Topic

While physical harms, or even emotional harms, to research subjects garner a lot of attention, issues related to privacy and confidentiality are much more common and can also lead to harms related to insurability, reputation, criminal or legal liability, stigmatization, social, financial, or employability, among others. This is an issue for both biomedical and social science research. No persons should be exposed to risk of harm due to disclosure of their private information as a result of their participation in research. The key regulatory criteria for the approval of research involved is that "when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data" (45CFR46.111(a)(7); 21CFR56.111(a)). The definitions usually used in the IRB world come from the OHRP IRB Guidebook (1993). Privacy is defined in terms of a person having control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others. Confidentiality is the process of protecting an individual's privacy. It pertains to treatment of information that an individual has disclosed in a relationship of trust, with the expectation that this information will not be divulged to others without permission. In general terms, privacy deals with people, confidentiality deals with data or information. Several OHRP determination letters cite organizations for not obtaining sufficient information from investigators on protecting the privacy of participants and the confidentiality of information. While the regulations list these terms together in one criterion, they are different concepts, require different actions, and thus should be treated separately.

IRB applications should ask how investigators plan to provide for the privacy of the participants. Researchers must demonstrate both the plan and the resources to maintain privacy. For example, if the participants are interviewed, are the interviews conducted in private environments where others cannot hear? Or if a person volunteers for an AIDS study, the research site they attend should not be stigmatizing, such as signs telling everyone it is an AIDS clinic. For young children, the presence of parents might protect the child's privacy while for teenagers, not having the parents present might be appropriate.

Likewise, IRB applications should ask investigators how they plan to keep information confidential. This can be a complex question in this high-tech world. Investigators should consider various strategies to maintain confidentiality of identifiable data including storage, use, sharing, and transmission of data. Protections may range from password protected computers, physical security of computers (especially laptops), restrictions on use of storing data on flash drives or CDs to more technical protections like firewalls, encryption, virus and malware protection, or intrusion detection software. Most organizations have technical requirements for information security or the IRB may have its own requirements for research data and information. Either way, the IRB should know and apply these requirements to research they review. This is an area where IRB members must enhance their knowledge and/or the IRB may have a member or consultant with expertise in information security. For example, if the only risk for a study is disclosure of sensitive information, the research may be classified as expedited if "reasonable and appropriate protections are implemented so that risks related to invasion of privacy and breach of confidentiality are no greater than minimal."* Thus, IRB members need to be aware of what "reasonable and appropriate" measures are to protect the information.

While a lot of emphasis is placed on protecting electronic information, there also must be security associated with physical materials such as paper forms, CDs, tapes, etc. Appropriate protections might be locked file cabinets, locked doors with limited access and access cards.

When appropriate with highly sensitive information, investigators might consider (or IRBs might require) obtaining certificates of confidentially to afford more protection to data. Certificates of Confidentiality are issued by the National Institutes of Health or other entities such as the Department of Justice, and allow the researcher to refuse to disclose identifying information on research participants in any civil, criminal, administrative, legislative, or other proceeding, whether at the federal, state, or local level (e.g. subpoenas), unless the participant consents. Any researcher can apply to the NIH for a Certificate of Confidentiality, whether or not the research is federally funded. A researcher must disclose in the Informed Consent Form any circumstances in which the researcher would need to disclose identifying

information to departments of health or other authorities (e.g., if the participant reveals the presence of certain communicable diseases, child abuse or elder abuse, or imminent harm to self and others). While certificates of confidentiality appear to provide strong protections, some lawyers point out that it is unclear if the certificates would stand up to challenges by the courts. For more information: http://grants.nih.gov/grants/policy/coc/index.htm

The Health Insurance Portability and Accountability Act (HIPAA) also provide additional safeguards for protected health information (PHI) used for research by limiting its access and use. HIPAA requires an authorization form to release PHI to researchers, which can be combined with a research consent form. HIPAA also has strict rules on what information can be considered de-identified. IRBs may be involved with HIPAA if they act as the Privacy Board for the organization. Privacy Boards can also grant a waiver of authorization.

The consent form should accurately describe to the subject information concerning the confidentiality of their information. A required element of informed consent is "A statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained" (45 CFR 46.116(a)(5)). The FDA goes further and adds "and that notes the possibility that the Food and Drug Administration may inspect the records" (21CFR 50.25). It is also good practice to list other third parties who may access the records including sponsors, the institution, the IRB, and other appropriate entities which may be specific to the research.

Privacy and confidentiality are two of the most important issues IRB must deal with when reviewing research, because so many research protocols involve private information. The IRB must have the expertise to evaluate information security plans in order to evaluate whether the regulatory criteria for approval are satisfied, and to provide potential subjects with the precautions that will be used to protect their personal information, so that they can make an informed decision whether to participate.

* OHRP Guidance: Expedited Review: Categories of Research that may be Reviewed Through an Expedited Review Procedure (1998)

Questions for the IRB to Consider

Questions your IRB may ask about privacy and confidentiality:

1. Has the investigator submitted adequate information to assess the plan to protect the privacy of subjects?
2. Is the privacy protection plan adequate, given the risks involved and the research protocol?
3. Has the investigator submitted adequate information to assess the plan to protect the confidentiality of data?
4. Is the confidentiality protection plan adequate, given the risks involved and the research protocol?
5. Do you or your IRB have the expertise to evaluate the information security plan?

IRB Decision: Are the privacy and confidentially protection plans adequate to satisfy the regulatory criteria for approval?

Case Studies

Case 1. A clinical investigator proposes a research project involving sexually transmitted infections, which includes conducting a sexual history interview with the subject in a hospital room. **What are your privacy concerns? What requirements would you necessitate?**

Case 2. An anthropologist loses a flash drive containing unencrypted identifiable data including some sensitive questions in an Amazon rain forest in South America. **What future requirements, if any, would you impose on the investigator in the current or future studies** (assuming you have already dealt with the issues as an unanticipated problem involving risks to participants or others)?

Case 3. A psychologist submits a protocol to survey 1000 women at a women's expo about issues related to child abuse and domestic violence. They wish to maintain identifiers in order to follow-up women who have been abused. **What reasonable and appropriate measures would you require to be able to categorize the research as expedited?**

Prospective Thinking: What are your information security requirements for:

- Laptops used in the field
- Sharing data through 1) email, 2) CDs, 3) flash drives, 4) a SharePoint site
- Encryption of sensitive information
- Passwords on desktop computers
- Data storage plans after a study is complete