Simplifying the Complexity of Confidentiality in Research

Journal of Empirical Research on Human Research Ethics
2015, Vol. 10(1) 100–102

DOI: 10.1177/1556264614568783
jre.sagepub.com
SAGE

Dear Practical Ethicist,

My IRB speaks of privacy and confidentiality in ways I do not understand. Sometimes people treat the two terms as interchangeable or synonymous. Sometimes they speak of each as a right, other times not. It seems that they treat privacy and confidentiality as words in everyday speech as though everyone should know what they mean. I'm not sure I really know what they mean. I'm also not sure whether they are rights that are guaranteed to us by some entity. Can you provide some clarity about these matters and what it means for the IRB to consider privacy and confidentiality?

Confused

Dear Confused,

Confidentiality can appear to be a complicated topic. With the advent of electronic medical records and the development of large databases, an increasing number of research studies are being proposed that involve the extensive collection and use of data, and the ethical risk of these protocols is breach of confidentiality. Confidentiality sounds complicated until you break down its components. Once the components of confidentiality are understood and considered individually, the complex becomes simple.

Definitions

In the context of research, *confidentiality* is the agreement to limit access to a subject's information. A requirement for confidentiality may exist because of a promise made by a researcher, an expectation of a subject (e.g., that medical records are confidential), or a legal requirement (e.g., Health Insurance Portability and Accountability Act [HIPAA]). In research, we commonly pledge to limit the dissemination of information about the subject to those with a need to know and to not divulge information to those without a need to know. This is a promise of confidentiality.

Confidentiality is different from privacy. Confidentiality concerns agreements about how data are handled, whereas privacy is about people and their desire to limit access to themselves in ways that may or may not involve information. One way to think about it is that confidentiality applies to data, whereas privacy applies to people.

Ethical Principles and Regulatory Criteria

The first simplification for understanding confidentiality issues in research is to realize that confidentiality affects two ethical principles of research: *respect for persons* and *beneficence*. Based on the ethical principle of respect for persons, we should explain to the subject our promises regarding limiting access to the subject's information and then abide by those promises. We also know that breaches of confidentiality can lead to risk of harm. Based on the ethical principle of beneficence, we should avoid that risk.

Based on these ethical principles, we should require procedures that eliminate *any* possibility of a breach of confidentiality. Unfortunately, the best laid plans can reduce the possibility of a breach to only a virtual, never an absolute, zero. The way to ensure that there is never a breach of confidentiality is to never do research, which would be even more costly and unethical.

The second simplification is to understand that confidentiality considerations affect four of the criteria for approval, specifically:

- Risks to subjects are minimized by using procedures that are consistent with sound research design and that do not unnecessarily expose subjects to risk.
- Risks to subjects are reasonable in relation to anticipated benefits, if any, to subjects, and the importance of the knowledge that may reasonably be expected to result.
- When appropriate, there are adequate provisions to maintain the confidentiality of data.
- Unless informed consent is waived or altered, subjects will be provided
  - a description of any reasonably foreseeable risks or discomforts to the subject, and
  - a statement describing the extent, if any, to which confidentiality of records identifying the subject will be will be provided to each subject.

Estimating Risk of Breach of Confidentiality

Before considering the criteria, the Institutional Review Board (IRB) should ascertain the facts, conduct a risk analysis, and understand procedures that mitigate the risk of a breach of confidentiality. What data will be gathered? Who will have access to the data? And how will the data be stored and protected?

When there are difficult confidentiality issues in a research study, the IRB's discussion may move among these four criteria without resolving any one. Typically, agreement is reached when consensus is realized on one criterion, although the other three may not be adequately addressed. When a debate ends with "We are not happy with this research, but as long as the consent document is completely transparent regarding the risk of a breach of confidentiality, we are OK," you can be fairly certain that this has occurred. The solution is to consider the criteria sequentially; it may organize the debate if the IRB takes separate votes on each of the four criteria.

Risk has two components: probability of occurrence and magnitude of harm. The IRB should understand what informational harms may occur and then estimate the probability and magnitude of those harms. Magnitude can be assessed by considering the type of information being collected. Is the information about the subject's fast food preferences, the subject's terrorism activities, or something in between? Assessing the probability of harm requires discipline. As most people do, IRBs tend to overestimate the probability of unfamiliar events occurring, and to rely on gut impressions rather than on hard data (Janofsky & Starfield, 1981; Klitzman, 2013) A useful way to calibrate risk has been developed by Rid, Emanuel, and Wendler (2010).

The probability and magnitude of harms can be compared with published statistics on the probability and harm of a breach of confidentiality in daily life. For example, according to the Bureau of Justice, about 7% of readers of this column have been victims of identity theft (Harrell & Langton, 2013) Contrast this with the probability of a breach of health information protected by following HIPAA standards. The Office of Civil Rights reports about 2,500 incidents per year among all HIPAA covered entities nationwide (Office of Civil Rights, Health Information Privacy, 2014) If a research database is protected by the same standards used by a health care entity covered by HIPAA, the probability of a breach is much less than the risk of a breach in daily life and reasonably represents a minimal risk standard.

Determining Whether the Level of Risk to Confidentiality Is Acceptable

Returning to the specific criteria, how should the IRB apply the criteria for approval to confidentiality? As noted before, the IRB should consider each criterion sequentially, focus on one criterion at a time, and resolve that criterion before moving on. If a criterion is not met, the research is not approvable and there is no value in considering the remaining criteria.

- Risks to subjects are minimized by using procedures that are consistent with sound research design and that do not unnecessarily expose subjects to risk.
    - Is there another way to conduct the research that reduces risks and allows the research to meet its scientific aims? If the risk of a breach of confidentiality is no more than minimal, this criterion is met because minimal risk is minimized risk. If not, protecting the data with the same procedures the institution uses to protect data covered by HIPAA will keep risks minimal. In those rare cases where it is not possible to apply this standard without adversely affecting the science of the research, consultation with a data security expert is indicated.
- Risks to subjects are reasonable in relation to anticipated benefits, if any, to subjects, and the importance of the knowledge that may reasonably be expected to result.
    - If the only risk is that of a breach of confidentiality and that risk is no more than minimal, this criterion is met provided there is at least minimal benefit to subjects or minimal importance of knowledge expected to result. If the only risk is that of a breach of confidentiality and that risk is more than minimal, the IRB must make a judgment call to balance those risks against the benefits of the research.
- When appropriate, there are adequate provisions to maintain the confidentiality of data.
    - The question for the IRB is whether the investigator (including research staff and others who could conceivably breach confidentiality) will likely abide by the promises made to the subject. This criterion is not about risk, but is about maintaining agreements with the subject. It is possible that the first two criteria are met, but the procedures to maintain confidentiality might be insufficient for the investigator to abide by the promises made. Either the procedures to protect the data need to be strengthened or the promises made to subjects need to be relaxed.
- Unless informed consent is waived or altered, subjects will be provided a description of any reasonably foreseeable risks or discomforts to the subject, and a statement describing the extent, if any, to which confidentiality of records identifying the subject will be provided to each subject

- Subjects should be routinely informed that confidentiality cannot be absolutely guaranteed. There is no explicit requirement to describe the confidentiality procedures that will be followed (files will be in a locked cabinet, etc.). However, subjects should be told with whom the investigator intends to share data and from whom the investigator intends to withhold data.

In summary, confidentiality can appear complicated because it involves two of the three ethical principles governing human research and affects four of the criteria for approval. However, by systematically and sequentially considering the components of confidentiality and how they affect the research, complexity can be reduced to simplicity.

P. Ethicist

References

Harrell, E., & Langton, L. (2013). *Victims of identity theft, 2012*. Retrieved from http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4821

Janofsky, J., & Starfield, B. (1981). Assessment of risk in research on children. *Journal of Pediatrics*, *98*, 842-846.

Klitzman, R. L. (2013). How IRBs view and make decisions about social risks. *Journal of Empirical Research on Human Research Ethics*, *8*(3), 58-65.

Office of Civil Rights, Health Information Privacy. (2014). *Enforcement highlights*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/

Rid, A., Emanuel, E. J., & Wendler, D. (2010). Evaluating the risks of clinical research. *Journal of the American Medical Association*, *304*, 1472-1479.

Author Biographies

Dr. Practical Ethicist, in real life, is a collaboration of two experts: Jeffrey A. Cooper and Lindsay McNair. They can be reached at JCooper@wcgclinical.com and LMcNair@wcgclinical.com

Jeffrey A. Cooper, MD, MMM, is a physician, basic science investigator, clinical investigator, and manager with many years of ethical review experience as a member and chair of an IRB. He left medical practice in 2002 to help start the Association for Accreditation of Human Research Protection Programs, Inc. (AAHRPP), where he was responsible for the development and operation of the accreditation process. He is currently the vice president of Global Consulting at WIRB–Copernicus Group.

Lindsay McNair, MD, MPH, MSBioethics, is a physician, clinical investigator, and former academic IRB member who has spent most of her career working in clinical research for the pharmaceutical and biotechnology industry, with a specific interest in ethical drug development research. She is an adjunct faculty member at Boston University and is currently the chief medical officer and president of Consulting Services for the WIRB–Copernicus Group.